Passer og linjal, origami og Galoisteori

Masteroppgave i matematikk

Thomas Vasdal

Matematisk institutt, Universitet i Bergen

30. mai 2011

Innholdsfortegnelse

1. Innledning

"There is much to be said in favor of a game you play alone… the company is most congenial and perfectly matched in skill and intelligence, and there is no embarrassing sarcastic utterance should you make a stupid play. The game is particularly good if it is truly challenging and if it possesses manifold variety… The Greek geometers of antiquity devised such a game…"

Howard Eves (1911-2004)

I denne oppgaven skal vi se på noen geometriske "spill" eller geometriske problemer som har vært prøvd løst i tusener av år. Disse problemene har tiltrukket seg en enorm mengde med oppmerksomhet opp gjennom århundrene. Enkelte matematikere gikk rett og slett fra forstanden under arbeidet med disse.

I dette spillet er det bare lov å bruke passer og linjal for å løse problemene. Passer og linjal-konstruksjoner er trolig kjent fra geometrien i ungdomsskolen. Nå til dags blir slike verktøy som regel kun ansett som interessant i en ren skolekontekst. For de gamle grekerne og egypterne derimot var dette nyttige verktøy for blant annet byggeprosjekter og kartlegging. Problemene som en ønsket å løse med passer- og linjalkonstruksjoner var følgende: kubens fordobling, sirkelens kvadratur og vinkelens tredeling. Vi vil behandle disse i lys av Galoisteori. Til slutt vil jeg drøfte en annen type geometriske konstruksjoner som særlig Japan er kjent for, nemlig såkalt origami eller brettekonstruksjoner.

Det var ikke bare i fortiden at det var stor interesse for disse spørsmålene. Hvert eneste år bombarderes matematiske institutter verden over av tusenvis av "løsningsforslag" til disse problemene. Hvorfor? Én mulig årsak til det vil jeg nevne senere i oppgaven.

Et ønske og formål med denne oppgaven er at den skal være både interessant og leselig for en lærer med lektorkompetanse i matematikk.

1.1. Følg reglene!

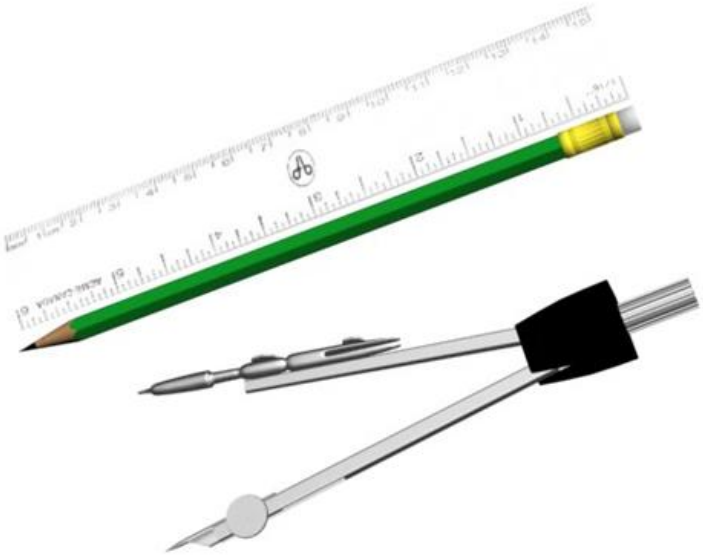
Grekerne som har hatt stor betydning for dagens moderne matematikk, greide ikke - selv så flink de var, å løse de tre klassiske problemene. De fant opp måter slik at de kunne løse de to første problemene nøyaktig, altså tredeling av vinkelen og kubens fordobling. For å gjøre dette måtte de bruke andre verktøy enn passer og linjal. Mange av dem som har "løst" ett av de klassiske problemene har kanskje uten å vite det brutt reglene:

- En kan bare bruke passer og en vanlig linjal.
- En kan ikke bruke linjalen til måling eller sette merker på den.

- En kan kun bruke passeren til å lage sirkler rundt et punkt, ikke ”bevege” passeren.
- En kan ikke bruke passeren og linjalen til å lage andre verktøy.
- En kan ikke bruke passeren og linjalen til å konstruere andre typer kurver.
- Alle smutthull eller forsøk på å unngå en av disse, er brudd på reglene.

”Passeren” og ”linjalen” i passer- og linjalkonstruksjoner er idealiseringer av passere og linjaler i den virkelige verden:

- *Passeren* kan åpnes vilkårlig bredt, men (ulikt noen virkelige passere) så har den ikke noen merker på seg. Den kan bare åpnes til bredder som allerede er konstruert.
- *Linjalen* er uendelig lang, men har ingen merker på seg og har dessuten bare én side (ulikt ordinære linjaler). Den kan bare brukes til å trekke linjer mellom to punkter eller å utvide en eksisterende linje.



Bilde 1 Passer og linjal

1.2. Hvorfor er man så opptatt av passer og linjal?

For å forstå hvorfor grekerne var så opptatt av passeren og linjalen, så kan en få noe innsikt i deres matematiske tenkning ved å betrakte Platons berømte allegori om hulen. I denne lignelsen sitter en fange i en hule og han kan kun få kunnskap om verden utenfor ved å betrakte skyggene på huleveggen. Hans kunnskap om verden utenfor er derfor forståelig nok ganske mangelfull. For mange grekere var denne verden eller vår oppfattelse av den, på samme måte. Den greske matematikeren anså linjene han tegnet som dårlige approksimasjoner av ”ekte linjer”, som var uendelig lange, uendelig skarpe, uendelig tynne og helt perfekt rett. Grekerne trodde at ”sannheten var der ute” i geometrien, de måtte bare finne den. Svaret eksisterte allerede og de ønsket å finne konstruksjoner som ville finne svaret uten feil med uendelig presisjon. Grekerne forkastet altså enhver teknikk som ble basert på

approksimeringer eller prøving og feiling. Problemet med prøving og feiling er at uansett hvor nært konstruksjonen ser ut til å passe, så kan vi aldri være sikker på at det ikke er en slags mikroskopisk feil utenfor vår oppfattelsesrekkevidde. Grekerne ønsket altså å finne det riktige punktet direkte, på første forsøk, med absolutt nøyaktighet [3].

Bilde 2 Platons hule lignelse

1.3. Referanser og valg av referanser

Jeg fant mye spennende stoff i verkene nedenfor. Audun Holme maler et levende bilde av den matematiske utviklingen som fant sted i oldtiden og det dramaet som utspant seg rundt det. Lesere som liker historie og matematikk oppfordres på det varmeste til å undersøke [2] og [5] nærmere! Nettadressen er også interessant og absolutt verdt et besøk. Nesten alle figurene i oppgaven er blitt laget ved hjelp av GeoGebra. GeoGebra er et flott læringsverktøy som både er gratis og lett å bruke.

(1) *Famous Mathematics Quotes*:

http://www.math.okstate.edu/~wli/teach/fmq.html

(2) Holme, A. (2008). *Matematikkens Historie 1*. Bergen: Fagbokforlaget.

(3) *Why Trisecting the Angle is Impossible*:

http://www.uwgb.edu/dutchs/pseudosc/trisect.htm

(4) *GeoGebra*:

http://www.geogebra.org/cms/en/installers

2. Klassiske problemer

"Circles to square and cubes to double would give a man exercise trouble"

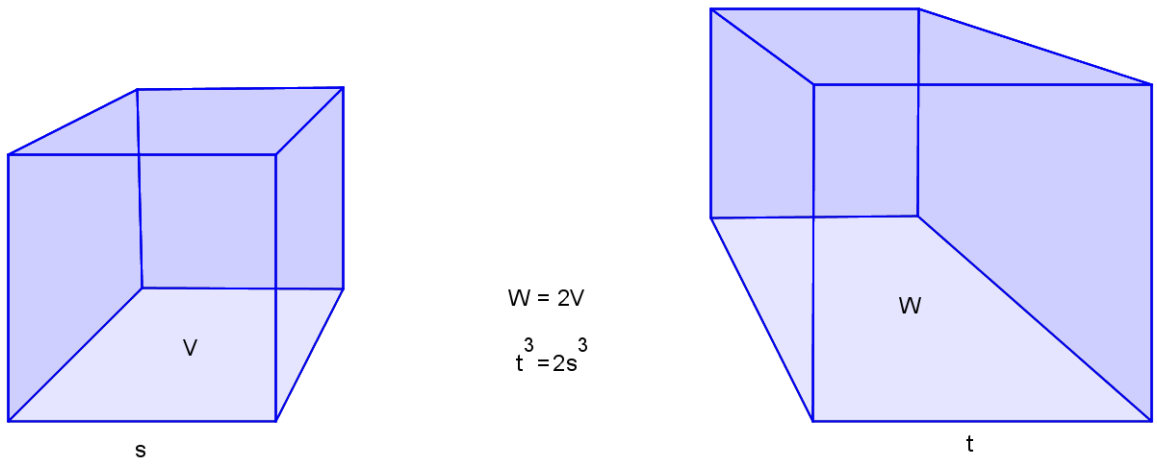
Matthew Prior (1664-1721)

Vi skal i den følgende delen gi en oversikt over de problemene vi ønsker og drøfte i denne oppgaven. Dette er problemer som har skapt og fortsatt skaper en enorm interesse. Disse oppgavene førte til mye nyskapning innenfor matematikken.

2.1. Kubens fordobling

Kubens fordobling: Gitt en kube med vilkårlig sidelengde, er det mulig ved bruk av passer og linjal å konstruere en kube med dobbelt så stort volum som den foregående kuben?

Det overnevnte kan kanskje høres litt utfordrende ut. Hvordan skal en konstruere en kube, som er en figur i rommet, med bare passer og linjal? Tanken er ikke at en bokstavelig skal konstruere en kube med passer og linjal. Idéen er bare å prøve å finne lengden av sidene til kuben med det dobbelte volumet, ved hjelp av passer og linjal.



Figur 1 Kubens fordobling

En mener at dette er et gammelt problem, muligens med røtter så langt tilbake som til det gamle Babylonia. Problemet er også kjent som det Deliske problem. Det er to versjoner av dette problemet. Den første lyder som følger: Da en pest raste som verst (pesten brøt ut rundt 427 f.v.t.)[1], sendte folk fra Athen en delegasjon til orakelet på Delos for å finne ut hva de skulle gjøre. Den deliske prestinnen

[1] I denne oppgaven vil jeg bruke "f.v.t." og "e.v.t." for henholdsvis "før vår tids regning" (altså før vår tidsregnings begynnelse) og "etter vår tidsregning" istedenfor "f.Kr" (før Kristus) og "e.Kr", se tillegget.

svarte: ”Apollons kubiske alter må fordobles”. Athenerne bygde da et alter som var dobbelt så høyt, bredt og langt, men pesten bare fortsatte. Athenerne forstod da at de ikke hadde fordoblet alteret, men åttedoblet det. Den andre versjonen går slik. Kong Minos var misfornøyd med det kubiske gravkammeret til sønnen Glaucus. Som i den første versjonen ønsket kongen at gravkammeret skulle dobles i størrelse, men han gav befaling om at alle dets sider skulle fordobles – som igjen gav en åttedobling.

Hippokrates (ca 470-410 f.v.t.) leverte et betydelig bidrag til dette problemet. Han tilbakeførte problemet til konstruksjon av en dobbelt mellomproporsjonal.

Bilde 3 Ruiner på Delos

2.1.1. Hippokrates bidrag

Hippokrates innsats i problemet med kubens fordobling, var altså at han sa at det var nok å kunne konstruere en dobbelt mellomproporsjonal[2]. Husk at problemet er som følger: Man har en gitt kube med sidekant lik linjestykket s og volum V. Konstruer med passer og linjal en ny kube med sidekant t og volum W som er dobbelt så stor som den forrige kuben. Dette betyr at $W = 2V$ som igjen impliserer at $t^3 = 2s^3$ (se ***Figur 1***).

[2] Se Tillegget for definisjon av enkel mellomproporsjonal

Den dobbelte mellomproporsjonalen er definert som følger; hvis a og b er kjente linjestykker, så prøver vi å finne linjestykkene α og β som er de to mellomproporsjonalene mellom a og b slik at:

$$a:\alpha = \alpha:\beta = \beta:b$$

$$\frac{a}{\alpha} = \frac{\alpha}{\beta} = \frac{\beta}{b}$$

La s være en side i en kube, der $b = s$ og $a = 2s$, da kan vi skrive:

$$\frac{2s}{\alpha} = \frac{\alpha}{\beta} = \frac{\beta}{s}$$

$$\left(\frac{\beta}{s}\right)^3 = \frac{2s}{\alpha} \cdot \frac{\alpha}{\beta} \cdot \frac{\beta}{s} = 2$$

Det betyr at:

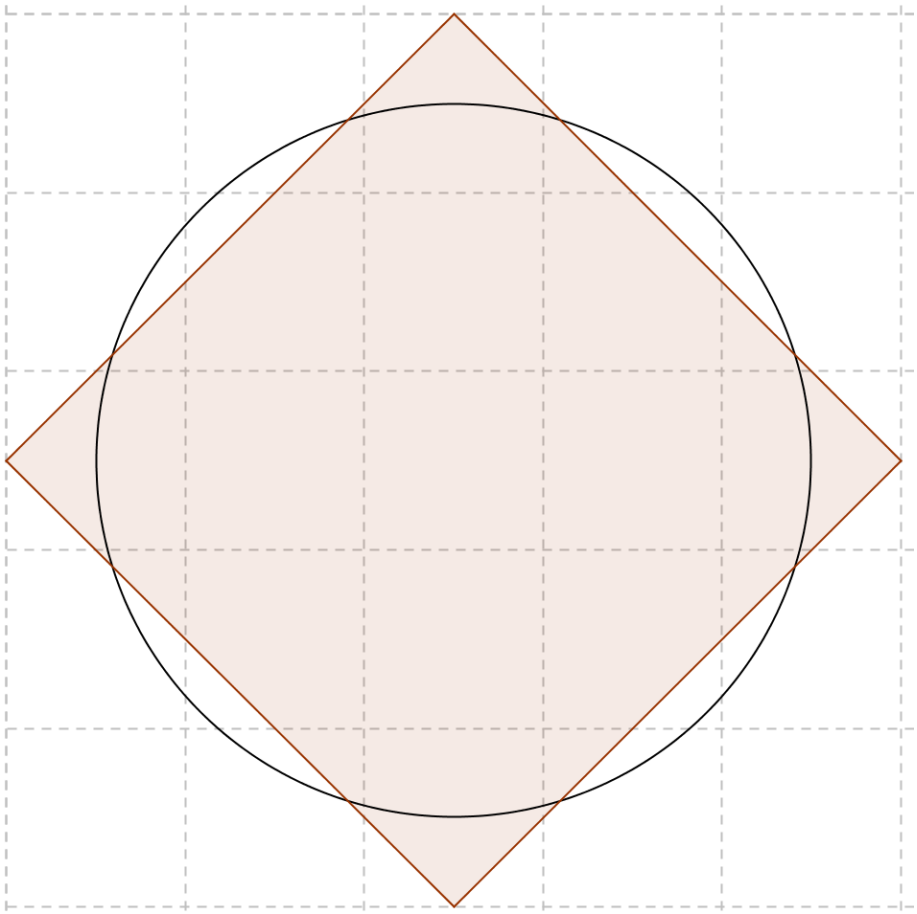
$$\beta^3 = 2s^3$$

Da vil altså en kube med β som lengde til sidene ha dobbelt så stort volum som en kube der s er lengden til sidene, som var det vi ønsket å konstruere. Poenget er altså at hvis den dobbelte mellomproporsjonalen er konstruerbar, da vil også kubens fordobling være det. Dessverre kan det vises at den dobbelte mellomproporsjonalen ikke er konstruerbar[3]. Se [2] kapitell 8.23 side 204.

2.2. Sirkelens kvadratur

Sirkelens kvadratur: Gitt en sirkel med vilkårlig radius, er det mulig med passer og linjal å lage et kvadrat med samme areal som den gitte sirkelen?

[3] Dette blir behandlet av Audun Holme i kapittel 3.8, side 59 i [5]. Her blir det også forklart hvordan vi med en enkel hjelpekonstruksjon kan konstruere den dobbelte mellomproporsjonalen, noe som selvfølgelig ikke er lov ifølge grekernes regler for passer og linjal.



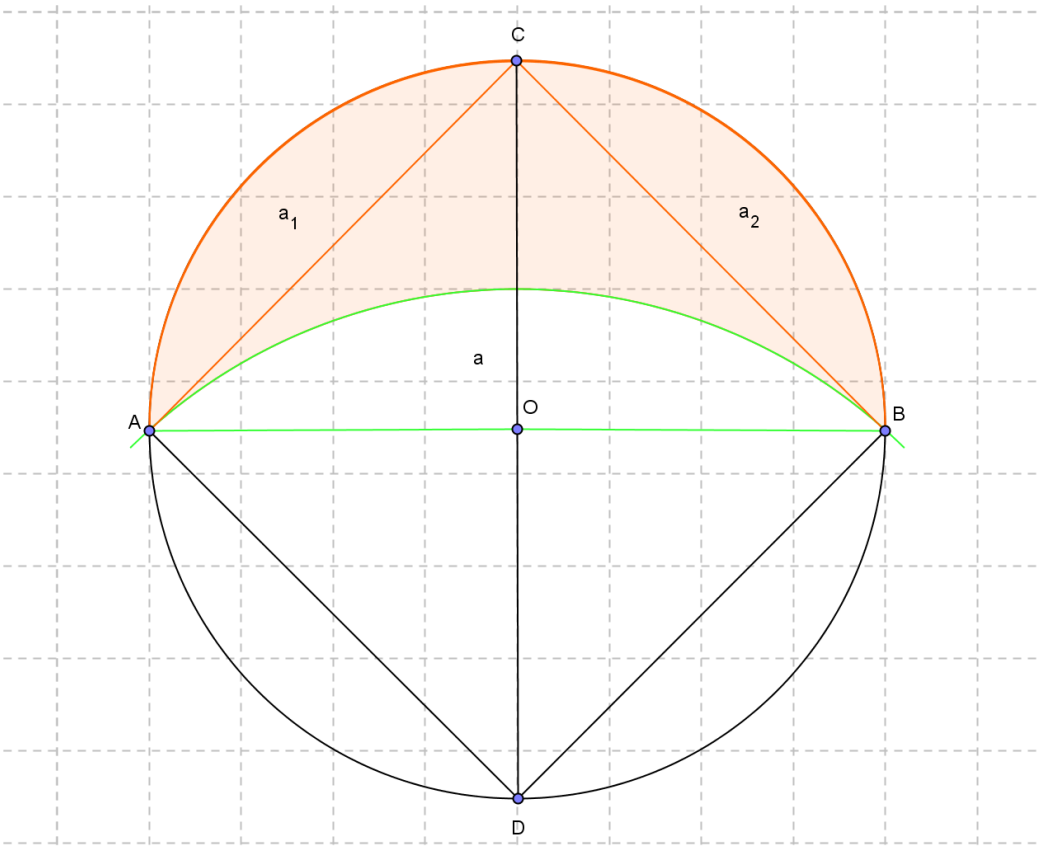
Figur 2 Sirkelens kvadratur

Hippokrates hadde omfattende geometriske kunnskaper, og foruten å arbeide med kubens fordobling, jobbet han også med sirkelens kvadratur. Han viste blant annet at enkelte spesielle måner lar seg kvadrere. Det skal vi se litt nærmere på nå.

2.2.1. Spesielle måner

På figuren under har vi tegnet inn en likebenet rettvinklet trekant ABC, der $AC = BC$, som igjen er innskrevet i en sirkel. Vi kaller arealet, som er avgrenset av linjen fra A til C og sirkelen, for a_1, og likeledes kaller vi arealet avgrenset av linjen mellom B og C og sirkelen, for a_2. Til slutt lar vi a være arealet avgrenset av linjen mellom A og B og en ny sirkel med radius AC og sentrum i D, slik at $ABCD$ danner et kvadrat.

Forholdet mellom radiene til sirklene kan skrives som $DA = \sqrt{2}OA$. Derfor vil sirkelen med sentrum i D ha dobbelt så stor areal som sirkelen med sentrum i O. Arealet a er formlikt med de to andre arealene $a_1$og a_2. Det betyr at forholdet mellom dem må være lik forholdet mellom arealene til sirklene. Da følger det at a må ha dobbelt så stort areal som enten $a_1$eller a_2, altså $a = a_1 + a_2$.

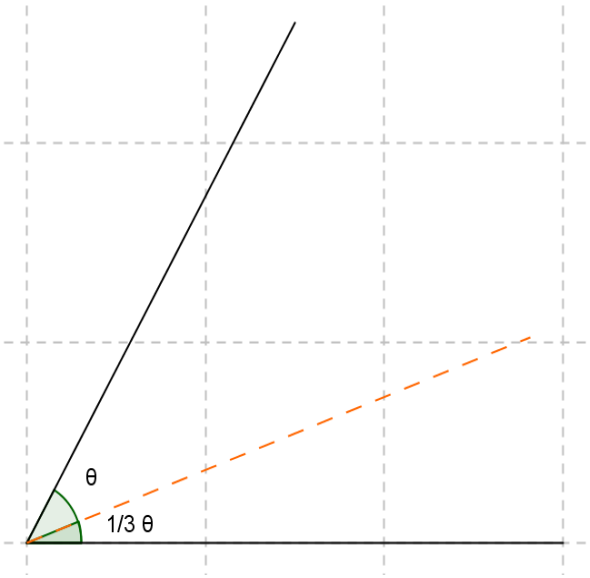


Figur 3 Enkleste spesielle måne som lar seg kvadrere

Ut fra figuren kan det kanskje virke som om det er mulig å kvadrere en sirkel. Det er jo ikke mye om å gjøre før denne månen blir en halvsirkel. Flere av Hippokrates kolleger tenkte slik. Hippokrates klarte ikke å kvadrere sirkelen, men han klarte derimot å kvadrere forskjellige måner. Dessverre klarte Hippokrates vel å merke ikke og kvadrere fullmånen eller halvmånen, noe som ville ha løst problemet! I kapittel 8.23 side 201 i [2], blir det vist hvordan en kan kvadrere mer kompliserte måner.

2.3. Vinkelens tredeling

Vinkelens tredeling: Et det mulig å dele en hvilken som helst vinkel i tre like store deler ved hjelp av passer og linjal?



Figur 4 Tredeling av vinkelen

En vet mindre om opprinnelsen til de to siste problemene enn det først nevnte problemet. Det kan muligens ha vært noe slikt: Det er enkelt å halvere og tredele et linjesegment med passer og linjal. Likeledes er det enkelt å halvere en vinkel. Dermed er det naturlig å undersøke om en kan tredele en hvilken som helst vinkel.

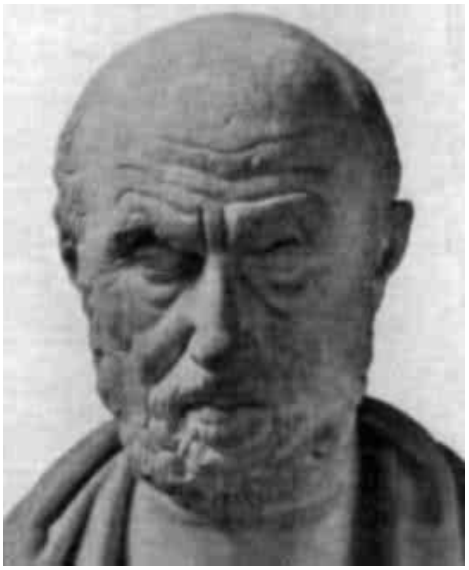
2.4. Hippokrates (ca. 470-410 f.v.t.)

Hippokrates[4] kom fra Kios, en øy utenfor kysten av Lilleasia. Hippokrates var en av pytagoreerne. Han var en dyktig geometer og han hadde noen gode ideer som fikk stor betydning senere. Hippokrates begynte ikke sin karriere som pytagoreer. Han var en kjøpmann som seilte rundt på Middelhavet og Svartehavet med sine varer. En gang ble Hippokrates plyndret av sjørøvere, og da han søkte nødhavn i Bysants tok tollerne resten av det han hadde igjen. Hippokrates mistet alt det han eide og kunne forståelig nok ikke fortsette i sin karriere som kjøpmann. Frustrert over de overnevnte banditten, reiste Hippokrates til Athen og prøvde å føre sak mot røverne og tollerne, men dette var ikke så enkelt. Han ble betraktet som både naiv og litt dum, som hadde latt seg plyndre og svindle på denne måten. Hvorfor Hippokrates søkte seg inn hos filosofene er uvisst, men det var trolig for å kunne få den nødvendige skoleringen. Hippokrates trengte skolering hvis han selv ønsket å legge fram sin sak i retten.

Geometri var en helt sentral del av grekernes utdannelse. Geometrien var sivilisasjonenes adelsmerke. En historie forteller om en gruppe reisende som led skipbrudd i Egeerhavet, og kom seg i land på en øy de ikke kjente. Fortvilet over situasjonen de var i, speidet de engstelig omkring stranden, da en av dem lettet utbrøt: ”Det er ingen fare! Jeg ser spor av siviliserte mennesker. Her er geometri risset inn i

[4] Må ikke forveksles med Hippokrates (460 - 377 f.v.t.) fra Kos, som blir omtalt som ”legekunstens far”.

sanden.". Hippokrates gjorde raske framskritt i geometrien, og overgikk snart sine lærere. Det er tydelig at Hippokrates ble høyt verdsatt for sitt arbeid. Pytagoreerne som gjerne ville at han skulle fortsette med sitt arbeid, var villig til å gi Hippokrates et meget sjenerøst tilbud. For å tjene inn igjen det han hadde tapt, skulle han få lov til å publisere bøker om pytagoreernes matematikk sammen med sitt eget matematiske arbeid. Hva hadde Hippokrates gjort for å få et slikt tilbud? Som vi har vært inne på før, mente de at han hadde gjort store framskritt for å løse problemet med sirkelens kvadratur. For mer detaljer, se kapittel 8.23 side 197 i [2].



Bilde 4 Hippokrates fra Kios

2.5. Referanser og valg av referanser

En kan finne en hel del spennende stoff og historie om og rundt de klassiske problemene i Holme sin "*Matematikkens Historie 1*". Der finner en også mye ekstra historie og detaljer rundt Hippokrates. Hvis en ønsker mer tekniske detaljer, som blant annet om den dobbelte mellomproporsjonalen, så anbefales "*Geometry: Our Cultural Heritage*".

(1) *Famous Mathematics Quotes*:

http://www.math.okstate.edu/~wli/teach/fmq.html

(2) Holme, A. (2008). *Matematikkens Historie 1*. Bergen: Fagbokforlaget.

(5) Holme, A. (2010). *Geometry: Our Cultural Heritage*. Bergen: Springer (Elektronisk)

(6) Cox, D.A. (2004). *Galois Theory*. New Jersey: Wiley

3. De konstruerbare tallene

"It is the glory of geometry that from so few principles, fetched from without, it is able to accomplish so much"

Sir Isaac Newton (1643-1727)

I dette avsnittet skal vi se nærmere på det moderne maskineri en kan bruke for å behandle de ovennevnte problemene. Vi starter med punktene 0 og 1. Hvilke nye punkter kan en konstruere ved bare å bruke passer og linjal? De fleste resultatene og bevisene i dette kapittelet er hentet fra [6] kapittel 10.1 sidene 255-261

3.1. Punkter vi kan konstruere med passer og linjal

I avsnitt 1.1 snakket vi litt om å følge reglene for passer og linjal. Nå vil vi gjerne gjøre det veldig klart hva vi egentlig mener med dette. Vi kan lage en liste over aksiomer som tydelig viser hva vi har lov til å konsturere med passer og linjal. Hvorfor ønsker vi å gjøre det? Hovedsakelig fordi vi ønsker å overføre problemet med passer og linjal om til et problem vi lettere kan manipulere med noe veldig fin matematikk som vi skal behandle siden. Fordelene med å gjøre det på denne måten, er enorme, noe som du snart vil få se.

K 1. Gitt to punkter $\alpha \neq \beta$ kan trekke en linje mellom punktene α og β.

K 2. Gitt tre punkter α, β og γ der $\alpha \neq \beta$ kan konstruere en sirkel med sentrum γ og radius Lik avstanden fra α til β.

P 1. Gitt to linjer $l_1 \neq l_2$ så er $l_1 \cap l_2$ et punkt.

P 2. Gitt en linje l og en sirkel s, så er $s \cap l$ punkter.

P 3. Gitt to sirkler $s_1 \neq s_2$ så er $s_1 \cap s_2$ punkter.

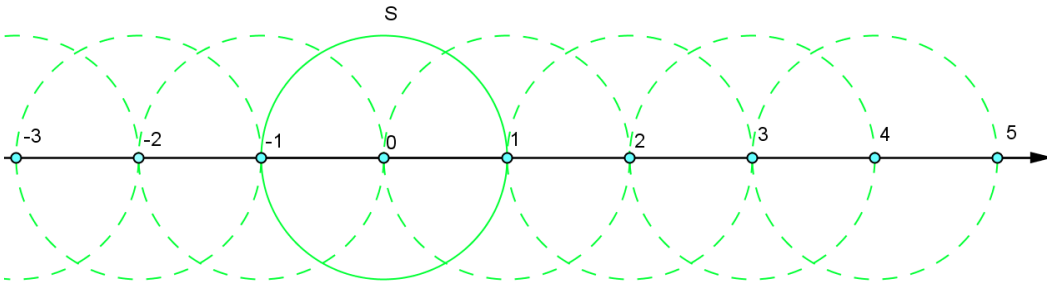
Her er det viktig at en er våken for en liten fallgruve! Fra våre tidligere erfaringer med linjer, så vet vi at en linje består av uendlig mange punkter. Da kan en kanskje tenke at hvis vi først har konstruert en linje (K 1), så vil alle punktene som linjen består av også være konstruerbare. Men dette er ikke riktig! Alle punktene er der, men bare noen er konstruerbare. Hvilke punkter er konstruerbare? Følgende definisjon gir oss svaret på det:

Definisjon 1.: La $\mathcal{k}$ være mengden av punkter (tall) i $\mathbb{C}$ som kan konstrueres fra punktene 0 og 1 ved å bruke K 1, K 2, P 1, P 2 og P 3 gjentatte ganger.

Legg merke til at K 1 og K 2 ikke gir nye konstruerbare punkter, bare P 1, P 2 og P 3 gjør det. La oss nå bruke denne definisjonen og aksiomene til å konstruere noen nye tall. Husk at målet vårt er å

omgjøre problemet fra passer og linjal over til et problem som er lettere å arbeide med.

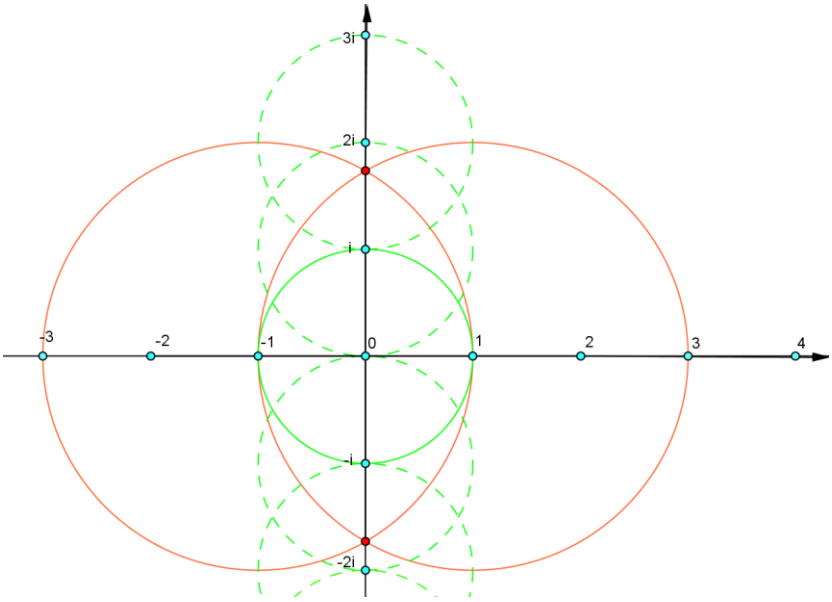
Eksempel 1.1.: Vi kan begynne med å konsturere heltallene (ℤ). Gitt to punkter 0 og 1 som er slik at en kan trekke en linje mellom dem (K 1), og slik at en kan konstruere en sirkel med sentrum i 0 og radius 1 som vil skjære i punktet 1 (K 2). Videre ser vi at sirkelen også vil snitte linjen i punktet -1 (P 2). Gjenta, men nå med sentrum i sirklene gitt som 1. Ved denne framgangsmåten kan en konstruere ℤ (Se ***Figur 5***).



Figur 5 Heltallene ℤ konstruert med passer og linjal

Vi kan altså konstruere heltallene, men kan vi konstruere noe mer spennende, for eksempel noen komplekse tall?

Eksempel 1.2.: For å kunne lage dette systemet, må vi kunne konstruere en normal i 0. Det kan vi gjøre på følgende måte (se ***Figur 6***):

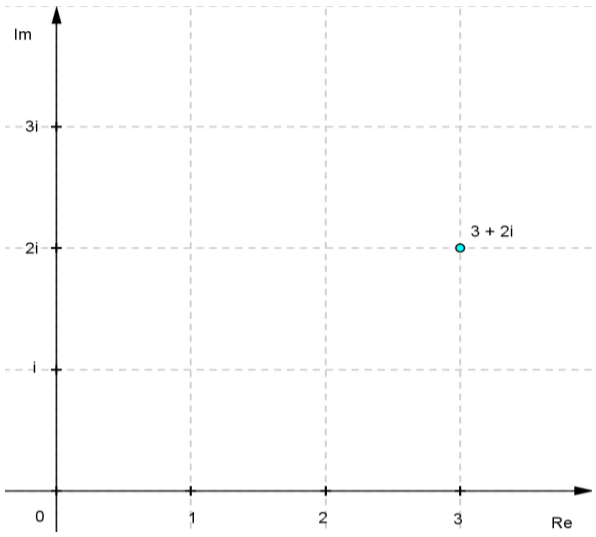


Figur 6 Konstruksjon av noen komplekse tall

Konstruer normalen ved å bruke K 2, der vi lar $\alpha = 1, \beta = -1 \; og \; \gamma = 1$ for den ene sirkelen, mens den andre får parameterene $\alpha = -1, \beta = 1 \; og \; \gamma = -1$. Da Får vi to skjæringspunkter ved P 3, og vi kan trekke en linje mellom punktene (K 1). Med samme framgangsmåte som i ***Eksempel 1.1.***, kan vi fylle ut den nye aksen med komplekse heltall.

Er det mulig å utvide vårt tallsystem? Hva hvis vi prøver å konstruere gitterpunkter i det komplekse planet? De gaussiske heltallene er nettopp det (Se ***Figur 7***). Er det mulig å lage de gaussiske heltallene bare ved hjelp av passer og linjal, altså vise at $\mathbb{k} \supseteq \mathbb{Z}[i]$?

Eksempel 1.3.: Husk at de gaussiske heltallene er definert ved $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$.



Figur 7 Et av de gaussisk heltallene

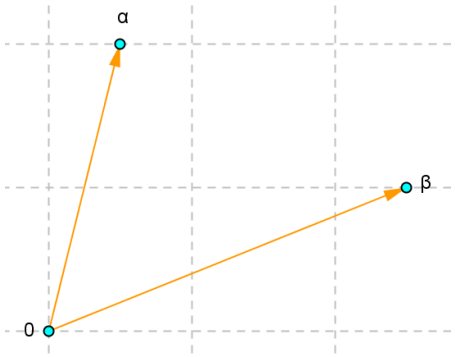
Hvordan skal vi så konstruere de gaussiske heltallene? Én måte å gjøre det på, er nokså lik måten som vi gjorde i ***Eksempel 1.2.*** – ser du hvordan? Vi skal imidlertid gjøre det på en litt annen måte. Følgende lemma vil ikke bare hjelpe oss til å konstruere de gaussiske heltallene, men også være til hjelp i vårt senere arbeid, nemlig arbeidet med å vise at $\mathbb{k}$ faktisk er en kropp.

Vi kan tenke på punktene vi konstruerer som vektorer. Det vil vise seg å være til stor hjelp for oss.

Lemma 1.: Antar at α og β er konstruerbare. Da vil $\alpha + \beta$ være konstruerbar.

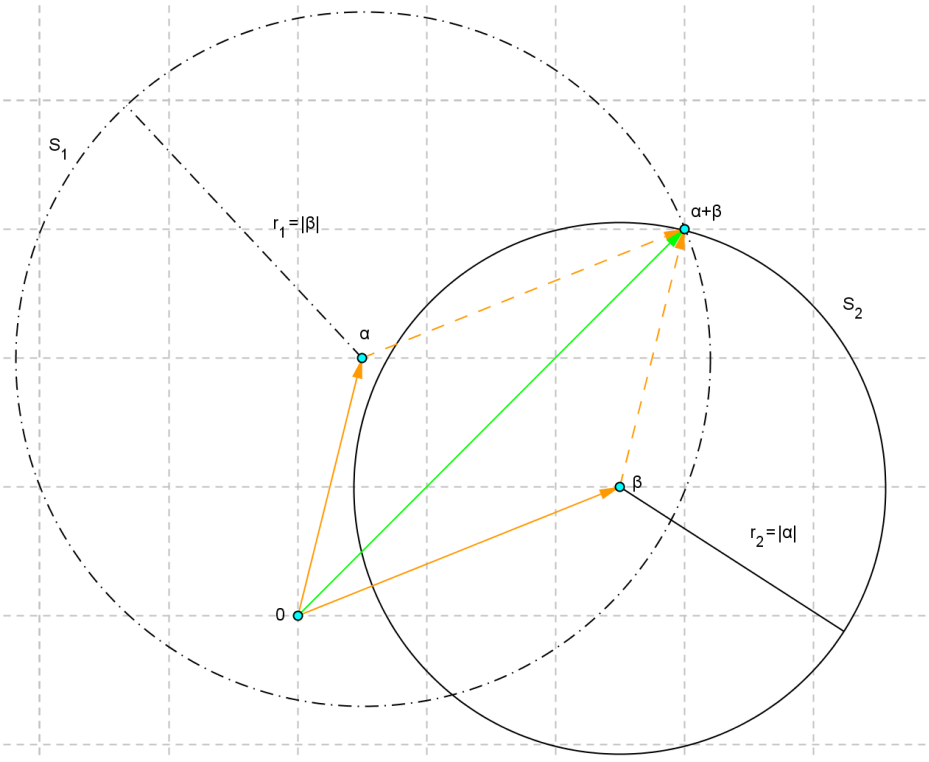
Bevis: Anta at vektoren α ikke er parallell med vektoren β

I ***Figur 8*** har vi tegnet inn de gitte vektorene.



Figur 8 Vektorene α og β

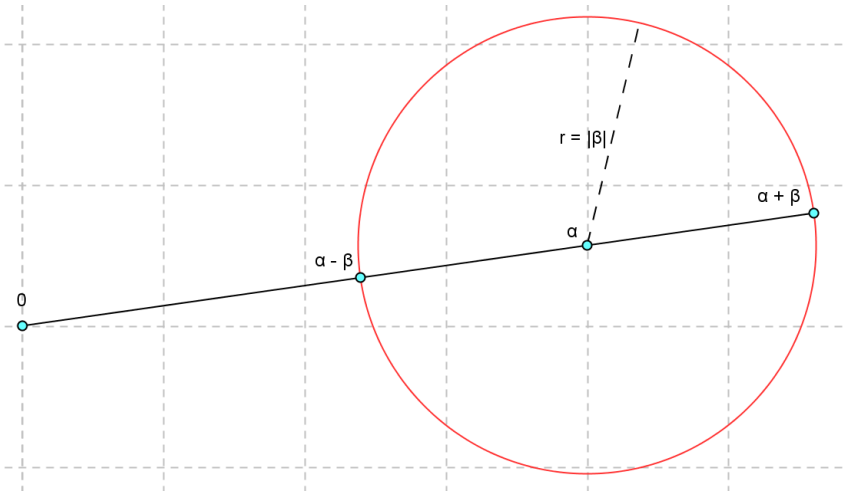
Vi husker at en kan dekomponere vektorer og dermed finne summen av vektorene. Kan man virkelig bare gjøre det med passer og linjal? Vi setter først passeren i punktet α og lager en sirkel S_1 med radius $|\beta|$ (K 2). Gjentar, men med passeren i punktet β med $|\alpha|$ som passerlengde og vi kaller sirkelen S_2. Vi får da to skjæringspunkt ved P 3. Skjæringspunktet som har vektorsummen $\alpha + \beta$, er det vi er interessert i. Dermed har vi funnet at $\alpha + \beta$ er konstruerbart når vektorene ikke er parallelle (se ***Figur 9***).



Figur 9 Konstruksjon når vektorene ikke er parallelle

Anta at vektoren α er parallell med vektoren β

Punktene 0, α og β er altså gitt, lager en linje gjennom 0 og α. Konstruerer en sirkel med sentrum i α og radius |β|. Ved P 2 får vi to skjæringspunkter. α + β og α − β er følgelig konstruerbar.



Figur 10 Konstruksjon når vektorene er parallelle

■

Det neste resultatet vil vise seg å være et viktig verktøy for vårt videre arbeid med å vise at $\hbar$ danner en kropp.

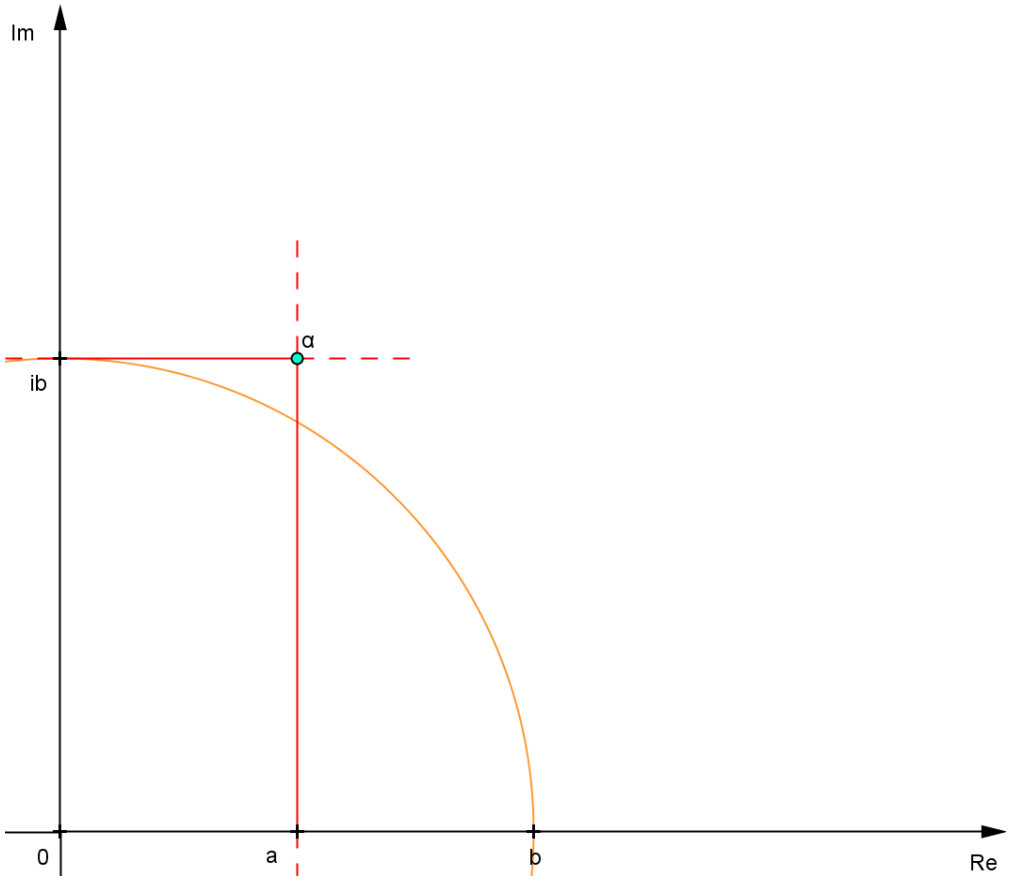
Lemma 2.: $\alpha = a + ib \in \hbar \; der \; a, b \in \mathbb{R} \Leftrightarrow a \; og \; b \; \in \hbar \cap \mathbb{R}$

Bevis: (⇒) Anta at $\alpha = a + ib \in \hbar$.

Nedfeller normaler fra α på den reelle og komplekse aksen, så har vi vist at $a, ib \in \hbar$. Sirkelen gitt ved $\gamma = 0$, $\alpha = 0$ og $\beta = ib$ (K 2) snitter den reelle aksen i b. Ved K 2 og P 2 har vi at $b \in \hbar$ (Se ***Figur 11***).

(⇐) Gitt $a \; og \; b \; \in \hbar \cap \mathbb{R}$.

Som i forrige del bruker vi K 2 og P 2 på sirkelen med radius $|b|$ og sentrum i 0. Dette viser at ib er konstruerbar. Da a og ib altså er konstruerbare, og ifølge ***Lemma 1.*** er $a + ib$ også konstruerbart.



Figur 11 Konstrukasjon av komponentene til α

■

Vi lyktes i å konstruere gitterpunkter, ettersom vi viste at $\alpha + \beta$ og $\alpha - \beta$ er konstruerbart. Men hvis vi nå ønsker oss punkter av typen $\frac{\alpha}{\beta}$ der $\alpha, \beta \in \mathbb{Z}[i]$, altså punkter i $\mathbb{Q}[i]$, kan disse også konstrureres? I Algebrakurset lærte vi at $\mathbb{Q}$ er en kropp[5]. Faktisk er det den minste kroppen vi har sammen med $\mathbb{Z}_p$. Vi vil altså vise at $\mathcal{k} \supset \mathbb{Q}[i]$. Hvis vi kan vise at $\mathcal{k}$ er en kropp, så følger det automatisk fra det vi vet så langt at $\mathcal{k} \supset \mathbb{Q}[i]$. Kan du forklare hvorfor?

3.2. Viktige resultater og bevis

På bakgrunn av det vi har drøftet, kan vi nå bevise følgende viktige teorem:

Teorem 1.: Mengden $\mathcal{k} = \{\alpha \in \mathbb{C} | \alpha \; er \; konstruerbar\}$ har følgende egenskaper:

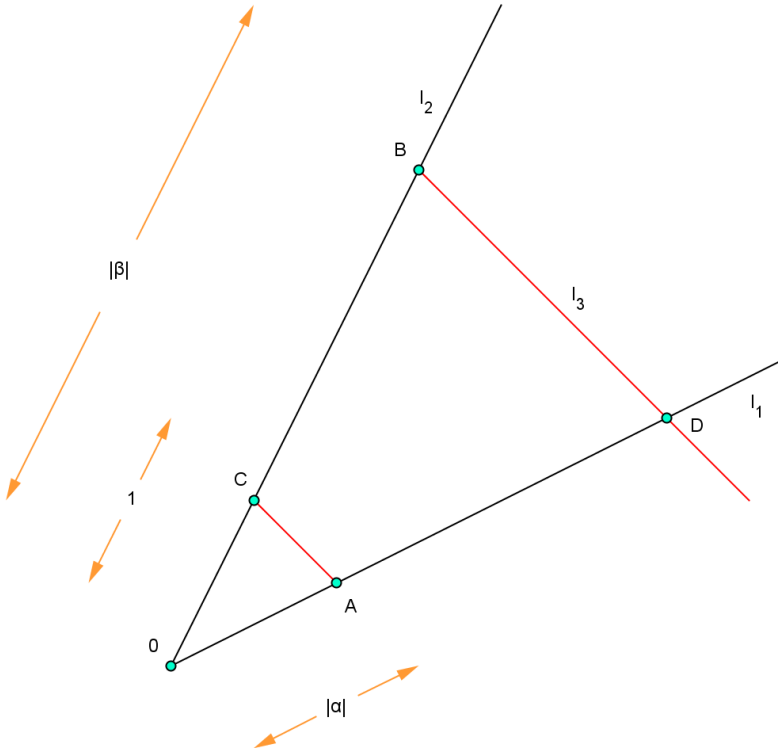
- $\mathcal{k}$ er en kropp.
- Hvis $\alpha \in \mathcal{k}$, så er $\sqrt{\alpha} \in \mathcal{k}$.

[5] I tillegget er det en del ekstra om kropper.

Bevis: $\hbar$ er en kropp

For å vise at $\hbar$ er en kropp, så må vi vise at kroppsaksiomene er oppfylte. Min påstand er at det er nok å vise at $\hbar$ er lukket under addisjon ($\alpha + \beta$), subtraksjon ($\alpha - \beta$), multiplikasjon ($\alpha\beta$) og divisjon (α/β), der α og β er konstruerbare! Hvorfor er det slik? La oss illustrere dette for assosiativitet av addisjon. Elementene α, β, γ i kroppen $\mathbb{C}$, vil som følge av assosiativitet kunne summeres i følgende rekkefølger: $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$. Hvis $\hbar$ er en delmengde av $\mathbb{C}$ og en bruker de samme operasjonene i $\hbar$ som i $\mathbb{C}$ og påstanden over er sann i $\mathbb{C}$, da må den være sann i $\hbar$ (når vi vet at $\hbar$ er lukket under addisjon). Dette er igjen sant ettersom en sjekker egenskapen for de samme elementene i $\mathbb{C}$, men muligens færre av dem. I en delmengde til en kropp vil altså de fleste av kroppsaksiomene være "arvet", slik vi illustrerte for assosiativitet.

I beviset av ***Lemma 1*** viste vi at $\hbar$ er lukket under addisjon og subtraksjon. Hva med $\alpha\beta$? Kan denne konstrueres? Konstruksjonen av $\alpha\beta$ er vist i ***Figur 12***. Vi lar $\overline{OA}$ være linjesegmentet fra 0 til A med lengde $|\alpha|$ på linjen l_1. Konstruerer linjen l_2, der $l_1 \nparallel l_2$. Punktene C og B på l_2 konstrueres slik at $\overline{OC}$ har lengde 1 og $\overline{OB}$ har lengde $|\beta|$. Trekker linjen $\overline{AC}$ og konstruerer linjen l_3 som er parallell med $\overline{AC}$ og går gjennom punktet B. Linjen l_3 skjærer l_1 i punktet D.



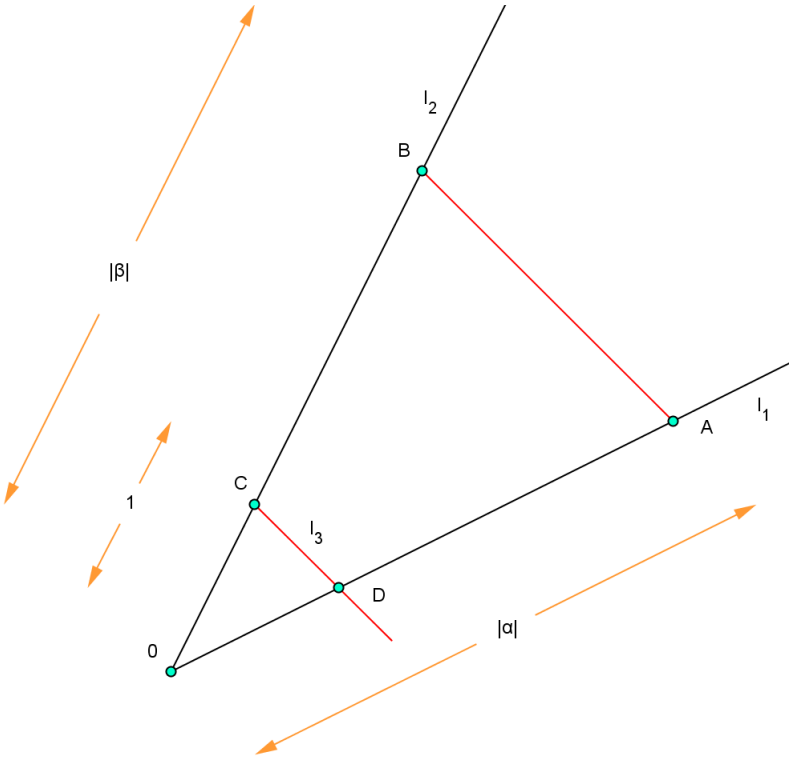
Figur 12 Konstruksjon av $\alpha\beta$

Vi ser at dette er to formlike trekanter. Dermed har vi at:

$$\frac{|\alpha|}{1} = \frac{|\overline{OD}|}{|\beta|} \Leftrightarrow |\overline{OD}| = |\alpha\beta|$$

Linjesegmentet $\overline{OD}$ har lengde $|\alpha\beta|$. Punktet αβ er konstruerbart ettersom dette bare er produktet av lengdene $|\alpha||\beta|$ og summen av argumentene til α og β, (summen av argumentene kan konstrueres ved å bruke enhetssirkelen).

Hva så med α/β? Nå må naturlig nok $\beta \neq 0$. Gjenta som i forrige konstruksjon, men nå trekker vi linjen $\overline{AB}$ og konstrurer linjen l_3 som er parallell med $\overline{AB}$ og går gjennom punktet C. Skjæringen $l_1 \cap l_3$ gir punktet D.



Figur 13 Konstruksjon av $|\alpha/\beta|$

Igjen får vi fra formlike trekanter:

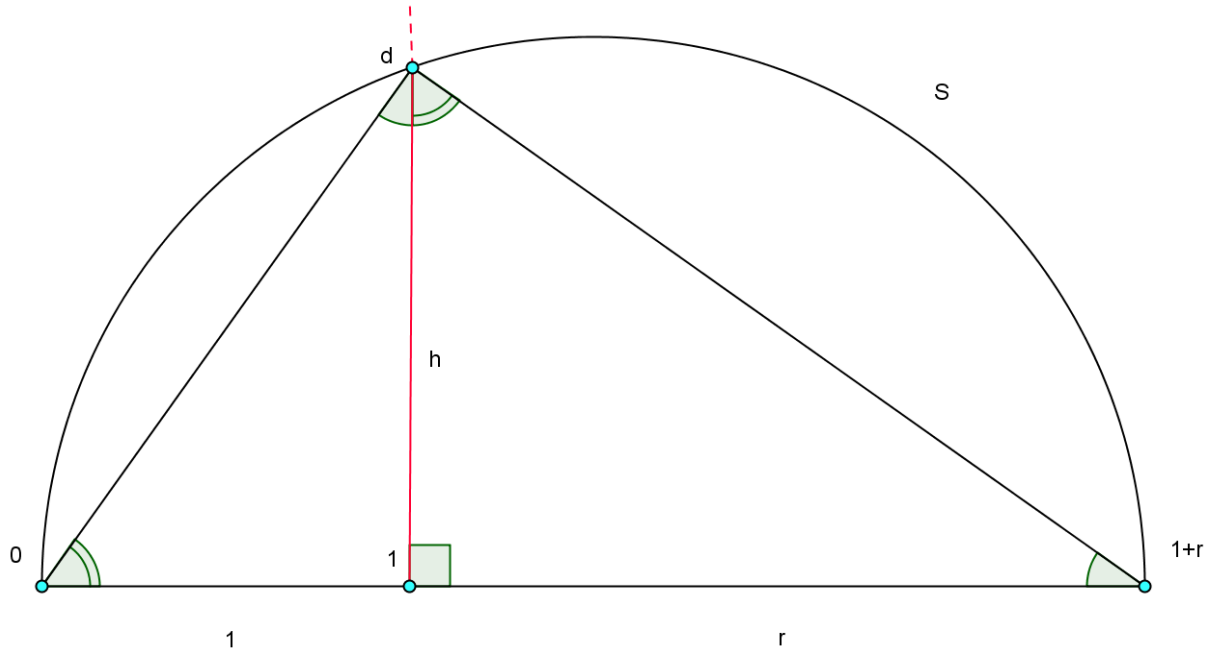
$$\frac{|\overline{OD}|}{1} = \frac{|\alpha|}{|\beta|} \Leftrightarrow |\overline{OD}| = \left|\frac{\alpha}{\beta}\right|$$

Det følger at punktet $\frac{\alpha}{\beta}$ er konstruerbart. Dermed vil de konstruerbare tallene danne en kropp.

Så vil vi gjerne vise at hvis $\alpha \in \mathbb{k}$, da er $\sqrt{\alpha} \in \mathbb{k}$.

Hvis vi kan skrive vårt ønskede punkt i polarkoordinater, altså $\alpha = re^{i\theta}$, der $r = |\alpha| > 0$. Da er det nok å vise at $\sqrt{r}$ er konstruerbar, fordi $\sqrt{\alpha} = \sqrt{re^{i\theta}} = \sqrt{r}e^{i\theta/2}$ og vinkler kan jo halveres med passer og linjal.
r er konstruerbar, ettersom en sirkel med radius $|\alpha|$ med sentrum i 0 vil skjære $x - aksen$ i $\pm r$ (K 2). Ved P 2, så er r konstruerbar.
Hvis vi kan konstruere $\sqrt{r}$, da kan også en sirkel med radius $\sqrt{r}$ med sentrum i 0 konstrueres (K 2). Til slutt ved bruk av P 2 på denne sirkelen og vinkelen $\theta/2$, så får vi at $\sqrt{r}e^{i\theta/2}$ er konstruerbar.

Da gjenstår det bare å vise at $\sqrt{r}$ er konstruerbar. Er den det?
Konstruksjonen av $\sqrt{r}$ kan gjøres på følgende måte: Trekker en linje gjennom de gitte punktene 0 og 1. Konstruerer så punktet 1+ r på samme linje. Deretter finner vi midtpunktet (for eksempel ved å lage sirkler med lik radius i endepunktene og lage en normal gjennom skjæringspunktene til sirklene). Så kan vi lage en halvsirkel S fra midtpunktet vårt. Til slutt lager vi en normal i punktet 1, og som skjærer halvsirkelen S. Det nye punktet kaller vi for d (Se ***Figur 14***). Vi kaller lengden mellom punktet 1 og punktet d for h.



Figur 14 Konstruksjon av $\sqrt{r}$ ved hjelp av enkel mellomproporsjonal, der r er et positivt reelt tall.

Ved formlike trekanter:

$$\frac{h}{r} = \frac{1}{h} \Leftrightarrow h^2 = r \Rightarrow h = \sqrt{r}$$

Siden d er konstruerbar, følger det at $h = \sqrt{r}$ er konstruerbar.

Altså $\sqrt{\alpha} \in \mathcal{k}$ ■

I den første delen av ***Teorem 1.*** klarte vi å bevise at $\mathcal{k}$ er en kropp. Hvorfor er dette så fint? Når folk flest jobber med matematikk, som algebra og aritmetikk, så bruker de kroppsaksiomene. Kroppene tillater oss å gjøre alle de tingene som vi ofte tar for gitt. I en kropp er det lov å bruke de fire regneartene (addisjon, subtraksjon, multiplikasjon og divisjon). Dessuten har alle elementene multiplikative inverser. Hvorfor er dette bra? Vi kan da for eksempel løse lineære ligninger. Hvis en ønsker å løse ligninger i en ring (hvor vi ikke har multiplikative inverser), blir ting fort mer komplisert. En annen fin ting med kropper, er at de er kommutative. Generelt er ikke multiplikasjon i en ring kommutativ. Kommutativiteten tillater for eksempel bruken av binomialformelen ($(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$).

Som en liten forberedelse til beviset av vårt neste teorem, vil jeg gjerne si noe om hvorvidt grafen til en ligning er konstruerbar og noe om ligninger beskrevet av komplekse punkter. Ettersom det er linjer og sirkler som er våre verktøy (ifølge aksiomene), så er det ligningene til disse vi må studere. Linjen

beskrevet av den linære ligningen $3x + 2y = 11$, er konstruerbart ifølge ***Teorem 1***. Samme ligning, men bare skalert annereledes $\frac{3}{7}x + \frac{2}{7}y = \frac{11}{7}$, vil også beskrive en konstruerbar linje. Men hva hvis ligningen så slik ut: $y = \pi x$? Det viser seg at π ikke er et konstruerbart tall (se avsnitt 4.2), så linjen beskrevet av ligningen vil ikke være konstruerbar. Dette er fordi en linje må inneholde minst to konstruerbare punkter for å være konstruerbar. Med dette i tankene, ser vi da behovet for å normalisere ligningene. Vi kan normalisere ligningen $ax + by = c$, ved å kreve at $a, b, c \in \mathbb{R} \cap \mathcal{k}$.

Vi vil vise at hvis linjen l går gjennom $\alpha = u_1 + iv_1$og $\beta = u_2 + iv_2$, hvor u_1, v_1, u_2 og v_2 ligger i en underkropp $F_n \cap \mathbb{R}$, så vil l være definert ved ligningen $ax + by = c$ hvor $a, b, c \in F_n \cap \mathbb{R}$. Punktene $\alpha = u_1 + iv_1$og $\beta = u_2 + v_2$ i $\mathbb{C}$ kan betraktes som punkter i $\mathbb{R}^2$ der $\alpha = (u_1, v_1)$ og $\beta = (u_2, v_2)$. Da vil linjen l kunne skrives som $(u_2 - u_1)(y - v_1) = (v_2 - v_1)(x - u_1) \Leftrightarrow (v_1 - v_2)x + (u_2 - u_1)y = (v_1u_1 + v_1u_2 - v_2u_1 - u_1v_1)$. Ettersom F er en kropp, så kan linjen skrives på formen $ax + by = c$ hvor $a, b, c \in F_n \cap \mathbb{R}$.

Den normaliserte ligningen for en sirkel vil vi skrive på formen $(x - a)^2 + (y - b)^2 = c^2$, hvor $a, b, c \in \mathbb{R} \cap \mathcal{k}$. Gitt den kvadratiske ligningen: $x^2 + y^2 + 2a_1x + 2b_1y = c_1$, så kan vi ved å fullføre kvadrater se at $c_1 + a_1^2 + b_1^2 > 0$ for at grafen skal være en sirkel.

Antar (som med linjen) at de komplekse og reelle delene til punktene $\alpha \neq \beta$ og γ ligger i en underkropp $F_n \cap \mathbb{R}$. Vi vil vise at sirkelen med sentrum i γ og radius $|\alpha - \beta|$ kan beskrives av ligningen $x^2 + y^2 + 2ax + 2by = c$ hvor $a, b, c \in F_n \cap \mathbb{R}$. Vi ser på punktene $\alpha = (u_1, v_1)$, $\beta = (u_2, v_2)$ og $\gamma = (u_3, v_3)$ hvor $u_1, v_1, u_2, v_2, u_3, v_3$ ligger i underkroppen $F_n \cap \mathbb{R}$. Da vil sirkelen kunne beskrives som $(x - u_3)^2 + (y - v_3)^2 = \left(\sqrt{(u_2 - u_1)^2 + (v_2 - v_1)^2}\right)^2$. Hvis vi skriver dette ut, finner vi at $x^2 + y^2 - 2u_3x - 2v_3y = (u_2 - u_1)^2 + (v_2 - v_1)^2 - {u_3}^2 - {v_3}^2$. Ettersom F er en kropp, så kan ligningen skrives på formen $x^2 + y^2 + 2ax + 2by = c$ hvor $a, b, c \in F_n \cap \mathbb{R}$.

Det neste teoremet er det siste vi trenger for å kunne svare på de klassiske problemene. Legg merke til at vi er avhengig av det vi fant i ***Teorem 1.*** for å kunne bruke det neste teoremet, nemlig det faktum at $\mathcal{k}$ er en kropp.

Teorem 2.: La $\alpha \in \mathbb{C}$. Da er $\alpha \in \mathcal{k}$ hvis, og bare hvis, det finnes en følge av kroppsutvidelser

$$\mathbb{Q}[i] = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n \subset \mathbb{C}$$

Slik at $\alpha \in F_n$ og graden $[F_i : F_{i-1}] = 2$ for alle $1 \leq i \leq n$.

Bevis: Jeg vil her bare gi en skisse av beviset, der jeg vil prøve å forklare de viktigste idéene.

($\Leftarrow$) Vi skal altså anta at $\mathbb{Q}[i] = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n \subset \mathbb{C}$, hvor hver av disse utvidelsene er av grad 2, der $\alpha \in F_n$. Vi vet at $F_i = F_{i-1}(\sqrt{\alpha_i})$ for $\alpha_i \in F_i$ (Se ***Lemma 3***).

Vi vil bruke induksjon for å vise at $F_i \subset \mathcal{k}$ der $0 \leq i \leq n$. Første steget ($i = 0$) i induksjonsbeviset er ok fordi $\mathbb{Q}[i] = F_0 \subset \mathcal{k}$ ved ***Teorem 1***. Hva med det neste steget? Vil $F_1 \subset \mathcal{k}$? $\alpha_1 \in F_0$er konstruerbar, som igjen betyr at $\sqrt{\alpha_1} \in \mathcal{k}$ (***Teorem 1.***). Ettersom F_n er en kropp, så vil $F_1 = F_0(\sqrt{\alpha_1}) \subset \mathcal{k}$. La oss gjøre dette mer generelt. Anta nå at $F_{i-1} \subset \mathcal{k}$. Da vil $\alpha_i \in F_{i-1}$ være konstruerbar, som igjen betyr at $\sqrt{\alpha_i} \in \mathcal{k}$. Igjen medfører det at F_n er en kropp til at $F_i = F_{i-1}(\sqrt{\alpha_i}) \subset \mathcal{k}$. Dette viser at $F_n \subset \mathcal{k}$, slik at enhver $\alpha \in F_n$ er konstruerbar.

($\Rightarrow$) Nå vil vi gjerne vise at hvis $\alpha \in \mathcal{k}$ så medfører dette at det eksisterer en rekke av kvadratiske utvidelser $\mathbb{Q}[i] = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n$ som til slutt inneholder α, altså $F_n \ni \alpha$. For å gjøre det, kan en bruke induksjon over de N gangene vi må bruke P 1, P 2 og P 3 for å konstruere α.

Ved det første steget i induksjonen, altså $N = 0$ (vi har ikke enda gjort noen konstruksjon), da må α være et av de gitte punktene 0 eller 1. Det vil altså si at $F_n = F_0 = \mathbb{Q}[i]$ er tilstrekkelig.

(P 1 – snittet mellom linjer): konstruksjon av α ved $N > 0$ steg, hvor vi i siste steget bruker P 1. Det vil si at α er et skjæringspunkt mellom to linjer l_1 og l_2, hvor l_1 går gjennom to punkter i F_n og l_2 går gjennom to punkter i F_n. Antar at linjene går gjennom de komplekse punktene β, γ, δ og ε som er konstruert ved $\leq N - 1$ anvendelser av P 1, P 2 og P 3. Ifølge vår induksjonshypotese og ***Lemma 2***, så finnes det derfor kvadratiske utvidelser $\mathbb{Q}[i] = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n$ som inneholder både den komplekse og reelle delen av punktene β, γ, δ og ε. Da vet vi (fra kommentarene før beviset) at de normaliserte ligningene kan uttrykkes som: $ax + by = e$ og $cx + dy = f$, der $a, b, c, d, e, f \in F_n \cap \mathbb{R}$. Fra Lineæralgebrakurset husker vi at en kan finne krysningspunktet ved å løse ligningene samtidig ved hjelp av matriseligningen $\boldsymbol{Ax} = \boldsymbol{b}$. Ettersom vi vet at linjene krysser, så må det finnes en unik løsning for ligningsystemet. Cramers regel gir oss:

$x = \begin{vmatrix} e & b \\ f & d \end{vmatrix} / \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \frac{ed-bf}{ad-bc}$ og $y = \begin{vmatrix} a & e \\ c & f \end{vmatrix} / \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \frac{af-ec}{ad-bc}$. På grunnlag av at F_n er en kropp, vet vi at den er lukket under addisjon, subtraksjon, multiplikasjon og divisjon. Da følger det at α ligger i F_n.

(P 2 – snittet mellom sirkel og linje): Anta nå at konstruksjonen av α foregår ved $N > 0$ steg, hvor P 2 benyttes i det siste steget. Det vil si at α er et skjæringspunkt mellom en linje l og en sirkel s hvor l går gjennom to punkter i F_n og s har sentrum og radius i F_n. Vi ser at koeffisientene til de normaliserte ligningene som vi får ved å anvende K 1 og K 2 kan finnes i F_n (igjen ved kommentar over beviset og antakelse). En kan ved å løse ligningen for linjen ved for eksempel x og deretter ved en substitusjon av denne inn i ligningen for sirkelen, få en annengradsligning av y uttrykt ved de overnevnte koeffisientene. Da vil abc-formelen også bestå av de samme koeffisientene. Hvis dette rotutrykket er inneholdt i F_n, så betyr det at verdiene for y og dermed også verdiene for x ligger i F_n, og dermed ligger den reelle og komplekse delen av α i F_n (***Lemma 2***). Hva hvis røttene ikke er inneholdt i F_n? Husk at det verste som kan skje, er at $F_{n+1} = F_n(\sqrt{b^2 - 4ac})$. Da vil verdiene for y og x og dermed α ligge i F_{n+1}, som bare er en kvadratisk utvidelse av F_n.

(P 3 – snittet mellom sirkel og sirkel): Anta til slutt at konstruksjonen av α foregår ved $N > 0$ steg, hvor P 3 benyttes i det siste steget. Det vil si at α er et skjæringspunkt av to sirkler med sentrum og radius i F_n. Ved induksjonshypotesen og ***Lemma 2*** kan vi finne en kvadratisk utvidelse slik at koeffisientene til de normaliserte ligningene for sirklene ligger i F_n. Hvis vi tar differansen mellom ligningene til sirklene, så faller de kvadratiske leddene bort. Generelt får vi da:

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$$

Ettersom ligningene for sirklene er unike og disjungte, så kan vi se at differansen mellom ligningene er ulik 0. Dermed må ligningen over beskrive en linje, og ligningen er normal. Hvis vi kombinerer denne ligningen med ligningen for den ene sirkelen, så vil en oppdage at vi kommer tilbake til P 2 – tilfellet. En kan med andre ord redusere P 3 til P 2. Konkluderer derfor med at α ligger i F_n eller i en kvadratisk utvidelse av F_n.■

Nå vil vi bevise ett av de resultatene vi brukte i det foregående beviset. Beviset av lemmaet bygger på noen resultater som kommer senere i oppgaven.

Lemma 3: Anta at $F \subset L$ er en kroppsutvidelse av grad 2 og at karakteristikken til F er ulik 2, da gjelder:

a) $L = F(\alpha)$, hvor α er en rot av et irredusibelt polynom av grad 2.
b) Minimalpolynomet av α over F er separabelt.
c) $F \subset L$ er en Galois utvidelse med $Gal(L/F) \simeq \mathbb{Z}/2\mathbb{Z}$.
d) Det finnes en $\beta \in L$ slik at $L = F(\beta)$ og $\beta^2 \in F$.

Bevis:

a) Vi ser på et element α i L, hvor $\alpha \notin F$. Da vet vi at $F \subsetneq F(\alpha) \subseteq L$. Bruker det vi vet om disse utvidelsene (***Teorem 17***) :

$$[L:F] = [L:F(\alpha)][F(\alpha):F] \Leftrightarrow 2 = 2[L:F(\alpha)] \Leftrightarrow [L:F(\alpha)] = 1$$

Det betyr at $F \subsetneq F(\alpha) = L$. Men vi er ikke helt ferdig. Det gjenstår å vise at α er en rot av et irredusibelt polynom av grad 2. Vi vet at minimalpolynomet til α må ha grad 2. Da følger det at α er en rot av et irredusibelt polynom av grad 2.

b) La $f = a_0x^2 + a_1x + a_2$, hvor $a_0 \neq 0$. Da vil $f' = 2a_0x + a_1$. Ettersom karakteristikken til F er ulik 2, så vil f' være ulik 0 og ha grad 1. Siden f er irredusibel, så er dens eneste divisorer 1 og f. Det vil si at $g = \gcd(f, f')$ må være 1 eller f. Men $g|f'$ og f' er ulik 0 impliserer at $\deg(g) \leq \deg(f') = 1$. Da kan ikke g være en multippel av f, slik at $\gcd(f, f') = g = 1$. Ifølge ***Teorem 5*** er f separabelt.

c) Ettersom L er en splittekropp av vårt separable polynom, så betyr det ifølge ***Definisjon 7*** at $F \subset L$ er en Galois-utvidelse. Videre kan vi bruke det fine ***Teorem 7.*** Vi vet jo at $[F(\alpha):F] = 2$, derfor må $|Gal(F(\alpha)/F)| = [F(\alpha) : F] = 2$. Derfor vet vi (se tillegget) at $Gal(F(\alpha)/F) \simeq \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$.

d) Vi kan skrive det separable polynomet $a_ox^2 + a_1x + a_2$ om til formen $a_0(x-h)^2 + k$, hvor h og k er konstanter i F (ved å fullføre kvadrater). Polynomet har følgende røtter: $x = h \pm \beta$, der vi lar $\beta = \sqrt{(-(k/a_0))}$. Det betyr at $\beta \in L$ og $\beta^2 \in F$, da gjenstår det bare å vise at $L = F(\beta)$. For å vise det, så er det nok å vise at $[L:F(\beta)] = 1$. Ved tårnteoremet:

$$[L:F] = [L:F(\beta)][F(\beta):F] \Leftrightarrow 2 = 2[L:F(\beta)] \Leftrightarrow [L:F(\beta)] = 1$$

For β som i forrige punkt., la $a = \beta^2 \in F$. Da kan vi skrive $\beta = \sqrt{a}$. Dette viser at hvis F har karakteristikk $\neq 2$, så kan en få tak i enhver utvidelse av grad 2 av F ved å bruke kvadratrøtter.

Til slutt vil vi trekke ut to viktige konsekvenser av ***Teorem 2***, som viser seg å være alt vi trenger for å besvare de gamle spørsmålene.

Korollar 1.: $\mathcal{K}$ er den minste underkroppen av $\mathbb{C}$, som er lukket med hensyn på å ta kvadratrøtter.

Korollar 2.: Hvis α er konstruerbart, så er $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$, der $n \geq 0$.

En konsekvens av korollar 2, er at ethvert konstruerbart tall er algebraisk over $\mathbb{Q}$, og at graden av dens minimalpolynom over $\mathbb{Q}$, er en potens av 2.

3.3. Referanser og valg av referanser

Både David A. Cox og John B. Fraleigh er fine å lese hvis en ønsker å sette seg mer inn i dette fascinerende emnet. Fraleigh er kanskje ikke så detaljert som Cox, noe som kanskje kan være en fordel hvis en bare ønsker å få et overblikk over de viktigste idéene og framgangsmetodene.

(1) *Famous Mathematics Quotes*:

http://www.math.okstate.edu/~wli/teach/fmq.html

(6) Cox, D.A. (2004). *Galois Theory.* New Jersey: Wiley

(7) Fraleigh, J.B. (2003). *A First Course In Abstract Algebra.* Rhode Island:

Pearson Education

4. De endelige svarene på de klassiske problemene

"If only I had the theorems! Then I should find the proofs easily enough."

Bernard Riemann (1826-1866)

I denne delen skal vi se at teorien vi har utviklet så langt faktisk er nok for å kunne gi svar på de klassiske problemene. Husk at de følgende bevisene er kulmineringen av flere tusen års hardt arbeid med disse spørsmålene. Legg merke til hvor enkel og elegant bevisene er. Ikke glem at alt dette er mulig på grunnlag av at vi viste at $\mathbb{k}$ er en kropp! Dette i sin tur gav oss et arsenal av teorier for å kunne takle disse vriene spørsmålene. Se kapittel 32 sidene 295-298 i [7] og kapittel 10.1 sidene 261-262 i [6].

4.1. Kubens fordobling

Kubens fordobling.: Korollar 2 er et meget sterkt resultat. Vi kan nå bruke dette for å løse det klassiske problemet med kubens fordobling. La den første kuben ha lengde 1 på sidene. Da har denne kuben volum 1. Kuben med dobbelt så stort volum må da ha sider av lengde $\sqrt[3]{2}$. Kan dette tallet konstrueres? Vi vet at $\sqrt[3]{2}$ er et nullpunkt av det irredusible $x^3 - 2$ over $\mathbb{Q}$ (En kan se at denne er irredusibel, for eksempel ved Schönemann-Eisenstein kriteriet (*Teorem 14*) i Tillegget). Vi får følgende indeks:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

Ved korollar 2, så må vi ha:

$$3 = 2^r$$

Der r er et heltall. Men det finnes ingen slik verdi for r. Dermed er α ikke konstruerbart og denne kubens fordobling er umulig med lovlig bruk av passer og linjal.■

4.2. Sirkelens kvadratur

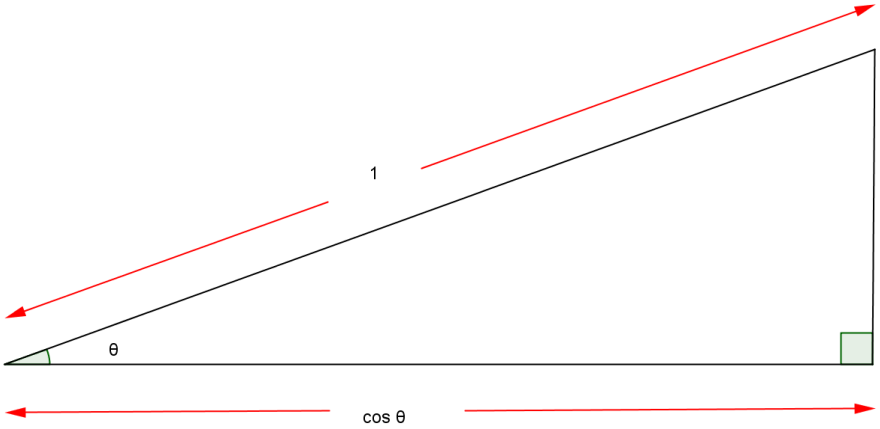
Sirkelens kvadratur.: Gitt en sirkel med radius 1. Da har sirkelen areal π. Kvadratet vi ønsker å konstrurere må ha en side med lengde $\sqrt{\pi}$. Men π er transedental over $\mathbb{Q}$[6], slik

[6] Det er velkjent at både π og *e* er transedental over $\mathbb{Q}$ (det betyr at π og *e* ikke er algebraisk over $\mathbb{Q}$). Det ble vist i 1882 av Lindemann, men dette er ikke lett å bevise.

at $\sqrt{\pi}$ også er transedental over $\mathbb{Q}$. Det vil altså si at det er umulig å kvadrere denne sirkelen (se kommentar etter *Korollar 2*). ■

4.3. Vinkelens tredeling

Vinkelens tredeling.: Figuren under indikerer at vinkelen θ kun kan konstrueres hvis, og bare hvis, et segment av lengde $|\cos\ \theta|$ kan konstrueres.



Figur 15 Vinkelen θ og $cos\theta$

Vi husker fra ungdomsskolen at 60 grader er konstruerbart. Kan denne vinkelen tredeles? For å svare på det spørsmålet vil vi utlede en trigonometrisk relasjon[7]:

$$cos3\theta = \cos(2\theta + \theta)$$
$$cos3\theta = cos2\theta cos\theta - sin2\theta sin\theta$$
$$cos3\theta = (2cos^2\theta - 1)cos\theta - 2sin\theta cos\theta sin\theta$$
$$cos3\theta = (2cos^2\theta - 1)cos\theta - 2cos\theta(1 - cos^2\theta)$$
$$cos3\theta = 4cos^3\theta - 3cos\theta$$

La $\theta = 20°$, da blir $cos3\theta = \frac{1}{2}$ og la $\alpha = cos20°$. Identiteten vi utledet over kan nå skrives som

$$4\alpha^3 - 3\alpha = \frac{1}{2}$$

[7] Her kunne vi også ha brukt Eulers formel for å utlede denne, altså $e^{ix} = \cos(x) + isin(x)$.

Dette kan vi skrive om til: $8x^3 - 6x - 1 = 0$. Dette polynomet er irredusibelt i $\mathbb{Q}[x]$, ettersom det ifølge ***Teorem 13*** er nok å vise at dette polynomet ikke har noen faktor i $\mathbb{Z}[x]$. En faktorisering i $\mathbb{Z}[x]$ vil innebære en lineær faktor på formen $(ax + b)$ hvor $a|8$ og $b| - 1$. Vi får følgende muligheter: $(8x \pm 1)$, $(4x \pm 1)$, $(2x \pm 1)$ og $(x \pm 1)$. Vi kan fort se at ingen av tallene: $\pm\frac{1}{8}$, $\pm\frac{1}{4}$, $\pm\frac{1}{2}$ og ± 1 er røtter av ligningen $8x^3 - 6x - 1 = 0$.
Dermed har vi ved det samme fine resultatet vi brukte på kubens fordobling:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3 \neq 2^r$$

α er altså ikke konstruerbart. En kan ikke tredele 60 grader med riktig bruk av passer og linjal. ■

Fellesnevneren for alle de klassiske problemene, er altså at de er uløselige.
Mange har vanskelig for å godta at noe i det hele tatt kan bevises å være umulig. Det kan være en forklaring på hvorfor matematiske institutter verden over hvert år får tilsendt så mange "løsningsforslag". Er ikke dette i seg selv en selvmotsigelse? Hvis en kan bevise at det er umulig å bevise at noe er umulig, da har en jo bevist at noe er umulig og dermed kommet med en selvmotsigelse. Faktisk så er det å kunne vise at noe medfører en selvmotsigelse et kraftig verktøy for å vise at enkelte ting er umulig, noe vi så flere eksempler på i disse avsnittene.

Bilde 5 Eksempel på selvmotsigelse

4.4. Referanser og valg av referanser

For en enkel og oversiktlig behandling av disse problemene, anbefaler jeg John B. Fraleigh sin bok. En forskjell mellom Fraleigh og Cox, er at Fraleig belyser disse problemene uten å gjøre bruk av de komplekse tallene.

(1) *Famous Mathematics Quotes*:

http://www.math.okstate.edu/~wli/teach/fmq.html

(6) Cox, D.A. (2004). *Galois Theory.* New Jersey: Wiley

(7) Fraleigh, J.B. (2003). *A First Course In Abstract Algebra.* Rhode Island:

Pearson Education

5. Galoisteori

"This letter, if judged by the novelty and profundity of ideas it contains, is perhaps the most substantial piece of writing in the whole literature of mankind"

Hermann Weyl (1885-1955)

Det overnevnte ble sagt om Évariste Galois matematiske testament. Galoisteorien er en fantastisk del av matematikken. Den har røtter så langt tilbake som den spennende historien om Tartaglia, Cardanos og Ferraris arbeid med tredje- og fjerdegradsligningene, fram til det tragiske dramaet om Évariste Galois og mot nyere tid. Galoisteorien gav oss mye mer enn bare en bedre forståelse av polynomets røtter og gripende drama. Den ble også en sentral del av fundamentet for mye av den moderne algebraen vi kjenner i dag, blant annet for grupper og kropper. Hvorfor er Galoisteorien så fin matematikk? En viktig grunn er at den viser forbindelsen mellom grupper og kropper. Galoisteorien blir ofte betraktet som en av de vakreste delene av matematikken. Se forordet side v i [6].

Bilde 6 Niccolò Fontana Tartaglia (1500-1557)

5.1. Évariste Galois (1811-1832)

Évariste Galois var en fransk matematiker som ble født den 25. oktober 1811 i Bourg-la-Reine. Selv i sitt alt for korte liv, gav Galois betydelige bidrag til matematikken. I tenårene fant han en tilstrekkelig og nødvendig betingelse for at polynomer skal være løselig ved rotutdragning, noe som hadde vært et stort problem opp gjennom tidene. Hans arbeid dannet også grunnlaget for Galoisteorien, som er en viktig del av den abstrakte algebraen. Han var også den første til å bruke ordet "gruppe" som et teknisk begrep i matematikken for å representere permutasjonsgrupper. Galois var meget politisk engasjert. Han var en radikal republikaner under monarkiet til Louis Philippe. Galois var bare 20 år gammel da han døde, som følge av skader han hadde pådratt seg i en duell.

Évariste Galois utmerket seg tidlig i sitt liv. I oktober 1823 begynte han ved det pristisjetunge Lycèe Louis-le-Grand skolen og klarte seg bra de første to årene, der han blant annet vant førsteplassen i en Latinkonkuranse. Han mistet etter hvert interessen for disse studiene og ble opptatt av matematikk. Allerede som 14 åring ble han seriøst interessert i matematikk. Han fant en kopi av Adrien Marie Legendre`s "*Èlèments de Gèomètrie*", som det sies at han leste som en novelle og mestret fult ut etter å ha bare lest den én gang. Som 15 åring leste han utgivelsene til Joseph Louis Lagrange, deriblant "*Rèflexions sur rèsolution algèbrique des èquations*", som trolig motiverte hans eget arbeid i ligningsteori. Foruten dette leste han også "*Leçons sur le calcul des fonctions*", som egentlig var myntet på profosjonelle matematikere!

Bilde 7 Galois som femtenåring, tegnet av en medelev.

Grunnene til at Galois havnet opp i den skjebnesvangre duellen, er ukjent. Galois var så sikker på utfallet av duellen, at han brukte hele natten til å skrive ned sine matematiske betraktninger i et brev, som skulle bli hans matematiske testament. En av de største matematikerene i det 20-århundre, Hermann Weyl, kommenterte dette testamentet med de flotte ordene som vi innledet dette kapittelet med. Tidlig om morgenen den 30. mai 1832, ble Galois skutt og døde dagen etter på Cochin sykehuset. Han var 20 år gammel, og hans siste ord til broren Alfred var:

"Ne pleure pas, Alfred! J'ai besoin de tout mon courage pour mourir à vingt ans!", som betyr
"Ikke gråt Alfred! Jeg trenger alt mitt mot for å kunne dø i en alder av 20 år".

Bilde 8 Minnesmerke om Galois i en kirkegård i Bourg-la-Reine.

Se kapittel 33 side 302 i [7]. For mer historie om Galois, se de historiske notatene i [6] og [7].

5.2. Splittekropper, normale utvidelser og separable polynomer

I dette avsnittet skal vi ta for oss litt av det bakgrunnsstoffet en trenger for å kunne benytte seg av Galoisteorien. Vi kommer til å se nærmere på kroppsutvidelser og noen viktige egenskaper til kroppsutvidelser. Resultatene er hentet fra kapittel 5.1-5.3 sidene 101-117 i [6].

Den første formen for kroppsutvidelser vi skal studere, er utvidelsen vi får når vi utvider kroppen med alle røttene til polynomet.

Definisjon 2.: La $f \in F[x]$ med grad $n > 0$. Utvidelsen $F \subset L$ er en *splittekropp* av f over F hvis:

- $\mathrm{f} = \mathrm{c}(\mathrm{x} - \alpha_1)(\mathrm{x} - \alpha_2) \cdots \mathrm{c}(\mathrm{x} - \alpha_\mathrm{n})$
- $\mathrm{L} = \mathrm{F}(\alpha_1, \alpha_2, \ldots, \alpha_\mathrm{n})$

Det neste teoremet vil fortelle oss om indeksen til disse kroppsutvidelsene. Resultatet gir en øvre terskel for kroppsutvidelsene.

Teorem 3.: La $f \in F[x]$ være et polynom med grad $n > 0$, og la L være en splittekropp av f over F. Da er $[\, L : F] \leq n!$

Å være en splittekropp, er en veldig spesiell egenskap til en kroppsutvidelse. Den neste definisjonen vil være viktig for den neste type utvidelser vi skal snakke om.

Definisjon 3.: La L være splittekroppen av $f \in F[x]$, og la $g \in F[x]$ være irredusibel. Hvis g har en rot i L, da vil g *splitte fullstendig* over L.

Fra algebraen husker du kanskje at normale undergrupper var viktige, blant annet for å konstruere faktorgruppen. Neste definisjon vil vise at det ikke bare er i gruppeteorien at en benytter begrepet normal.

Definisjon 4.: En algebraisk utvidelse $F \subset L$ er *normal* hvis hvert irredusibel polynom i $F[x]$ som har en rot i L splitter fullstendig over L.

Det er ingen tilfeldighet at begrepet *normal* forekommer både i gruppe- og kroppsteorien. I Galoisteorien vil vi få se grunnen til det. Det neste teoremet viser den nære sammenhengen mellom normale utvidelser og splittekropper.

Teorem 4.: Anta at $F \subset L$. Da er L splittekroppen av $f \in F[x]$ hvis, og bare hvis, utvidelsen $F \subset L$ er normal og endelig.

Vi skal nå se på et eksempel som vil gå som en rød tråd gjennom hele Galoisteorien. Jeg vil prøve å belyse noe av det stoffet vi har behandlet så langt.

Eksempel 2.1.: Vi begynner med å betrakte utvidelsen $\mathbb{Q}[\sqrt[3]{2}]$. Er dette en normal utvidelse av $\mathbb{Q}$?

Vi vet at $\sqrt[3]{2}$ har det irredusible polynomet $x^3 - 2$ (Her kan du sjekke på selv, for eksempel ved å bruke Schönemann – Eisenstein – kriteriet). Polynomet har 3 røtter, der 2 av disse er komplekse. Fra ***Definisjon 4.*** ser vi at røttene ikke splitter fullstendig over utvidelsen $\mathbb{Q}[\sqrt[3]{2}]$, (siden de komplekse røttene ikke kan leve i $\mathbb{Q}[\sqrt[3]{2}]$). Altså kan ikke $\mathbb{Q}[\sqrt[3]{2}]$ være er en normal utvidelse av $\mathbb{Q}$.

Selv om ikke alle utvidelser er normale, så er det alltid mulig å utvide disse slik at de blir normale. ***Eksempel 2.2.*** illustrerer det.

Eksempel 2.2.: La nå $\omega = e^{2\pi i/3}$. Vis at $L = \mathbb{Q}[\sqrt[3]{2}, \omega]$ er en normal utvidelse av $\mathbb{Q}$.

ω har konjugerte: ω^2 (***Teorem 15.*** i tillegget)
$\sqrt[3]{2}$ har konjugerte: $\sqrt[3]{2}\omega \; og \sqrt[3]{2}\omega^2$ (***Definisjon 16*** i tillegget)

Nå ser vi at røttene splitter fullstendig over utvidelsen vår, $L = \mathbb{Q}[\sqrt[3]{2}, \omega]$ fra ***Definisjon 4***.

Den neste delen av eksempel 2 forklarer hvordan vi kan finne graden til utvidelsen, altså indeksen $[L:\mathbb{Q}]$.

Eksempel 2.3.: La oss prøve å finne graden til utvidelsen $[L:\mathbb{Q}]$, der $L = \mathbb{Q}[\sqrt[3]{2}, \omega]$.

For å gjøre det skal vi se på utvidelsen $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{Q}[\sqrt[3]{2}, \omega] = L$.
Vi begynner med $[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}]$, som er irredusibelt over $\mathbb{Q}$ av grad 3. Deretter ser vi på utvidelsen $[L:\mathbb{Q}[\sqrt[3]{2}]]$. Det syklotomiske polynomet $x^2 + x + 1$, har de komplekse røttene ω og ω^2. Ettersom $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$, så har $x^2 + x + 1$ ingen røtter i denne kroppen. Det betyr at $x^2 + x + 1$ er minimal-polynomet av ω over $\mathbb{Q}[\sqrt[3]{2}]$. Altså $[L:\mathbb{Q}[\sqrt[3]{2}]] = 2$. Ifølge ***Teorem 17.*** så får vi utvidelsene: $[L:\mathbb{Q}] = [L:\mathbb{Q}[\sqrt[3]{2}]]\ [\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}] = 6$.

Det er viktig å innse at røttene til en funksjon med splittekropp L over F ikke alltid er unike. Funksjonen $f = x^2 - 2x + 1 \in \mathbb{Q}[x]$ *har røttene* $\alpha_1 = \alpha_2 = 1$. Vi vil i følgende definisjon være interessert i polynomer der alle røttene er ulike. Vi sier at en rot er *enkel* hvis den er unik. Hvis røttene ikke er unike kaller vi dem en *multippel* rot.

Definisjon 5.: Polynomet $f \in F[x]$ er *separabelt* hvis det ikke er konstant og alle dets røtter i en splittekropp er enkle.

Det neste resultatet er nyttig når en skal prøve å finne ut om et polynom er separabelt.

Teorem 5.: Hvis $f \in F[x]$ er monisk og ikke konstant, da er det følgende ekvivalent:

a) f er separabel
b) $\Delta f \neq 0$
c) f og f' er relativt primske i $F[x]$, det vil si at $\gcd(f, f') = 1$

5.3. Viktige teoremer og resultat i Galoisteorien

Endelig er vi klar til å ta fatt på selve Galoisteorien! Hvis du synes at enkelte deler av dette avsnittet eller andre deler av oppgaven kan være litt vanskelig å forstå, så kan du trøste deg med at du ikke er

den eneste som synes at slikt stoff er vanskelig! Kong Ptolemaios skal ha spurt Euklid[8] om det ikke fantes en enklere måte å lære geometri på. Euklid svarte med de berømte ordene ”Det finnes ingen kongevei til geometri”. Likeledes kan du være sikker på at det ikke finnes noen ”kongevei” til en bedre forståelse av verken geometri eller algebra.

Bilde 9 Statue av Euklid i Oxford universitets naturhistoriskmusuem

Vi skal begynne med å fortelle hva en automorfi egentlig er for noe, og deretter komme med vår første definisjon tilknyttet Galoisteorien. Husk at Kroppsutvidelser og automorfier er hele grunnlaget for vårt studie av Galois sin teori. Resultatene i dette kapittelet kan finnes i [6] kapittel 6.1-6.3 side 125-144 og kapittel 7.1-7.2 side 147-160.

Hvis L er en kropp, da er en *automorfi* av L kroppsisomorfien $\sigma: L \to L$. For en mer muntlig forklaring av begrepet automorfi, se ***Eksempel 7*** i tillegget.

Definisjon 6.: La $F \subset L$ være en endelig utvidelse. Da er $Gal(L/F)$ mengden

$$\{(\sigma: L \to L | \sigma \; er \; en \; automorfi, \sigma(a) = a \; for \; alle \; a \in F \;)\}$$

Dette betyr altså at $Gal(L/F)$ består av alle automorfiene av L som er identiteten på F.

[8] Euklid, også kjent som Euklid fra Alexandria (ca. 325-265 f.v.t.), var en matematikker i den greske kolonien Alexandria. Han blir ofte kalt for ”Geometriens far”.

Det viser seg at denne mengden av automorfier faktisk danner en gruppe, der gruppeoperasjonen er komposisjon[9].

Teorem 6.: $Gal(L/F)$ er en gruppe under komposisjon.

I det neste resultatet kommer noe av den teorien vi behandlet i forrige avsnitt fram. Det vil i sin tur medføre at vi kan bestemme indeksen til Galoisgruppen.

Teorem 7.: Hvis L er en splittekropp av et separabelt polynom i $F[x]$, da har Galoisgruppen av $F \subset L$ orden $|Gal(L/F)| = [L:F]$

Følgende teorem er et av de viktigste i Galoisteorien.

Teorem 8.: La $F \subset L$ være en endelig utvidelse. Da er følgende ekvivalent:

- L er en splittekropp av et separabelt polynom i F[x].
- F er den fikserte kroppen av Gal(L/F) som virker på L.
- F ⊂ L er en normal separabel utvidelse.

I lys av det overnevnte teoremet, skal vi definere en ny type utvidelse.

Definisjon 7.: En utvidelse $F \subset L$ blir kalt en *Galois- utvidelse* hvis det er en endelig utvidelse som tilfredstiller et av punktene i ***Teorem 8***

I den neste delen av eksempel 2, så skal vi virkelig begynne å jobbe med selve Galoisteorien.

Eksempel 2.4.: Bestem Galoisgruppen $Gal(L/\mathbb{Q})$.

$Gal(L/\mathbb{Q})$ er en gruppe av orden 6. Da vet vi at den må være $\mathbb{Z}_6$ eller S_3 (Se ***Tabell 5*** i tillegget). For å finne ut hvilke av disse det er, så undersøker vi om gruppen er abelsk.

Vi vet at: $\omega \mapsto \omega, \omega^2$ og $\sqrt[3]{2} \mapsto \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$
La oss dvele litt ved dette. Den lille pilen over betyr at elementet på venstre side blir sendt til et av elementene på høyre side. Hvis for eksempel

[9] Husk at komposisjon for funksjonene $f(x)$ og $g(x)$ skrives som $(f \circ g)(x) = f(g(x))$, som betyr at en setter funksjonen $g(x)$ inn i funksjonen $f(x)$.

f_2: $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$; $\omega \mapsto \omega$, der vi sier hva som skjer med to av elementene, så påstår vi at vi vet hva som skjer med alle elementene $(\omega, \omega^2, \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$. Hva skjer for eksempel med elementet $\omega\sqrt[3]{2}$? La oss se:

$$f_2\left(\omega\sqrt[3]{2}\right) = f_2(\omega)f_2\left(\sqrt[3]{2}\right) = \omega \cdot \omega\sqrt[3]{2} = \omega^2\sqrt[3]{2}.$$ [10]

Så $\omega\sqrt[3]{2}$ blir altså sendt til $\omega^2\sqrt[3]{2}$ av f_2. På samme måte kan en sjekke hvor de andre elementene blir sendt av funksjonen .

Nedenfor har vi listet opp alle mulighetene for hvor elementene kan bli sendt, og kalt de forksjellige funksjonene for $f_1, f_2, \dots, f_6$.

f_1: $\sqrt[3]{2} \mapsto \sqrt[3]{2}$; $\omega \mapsto \omega$

f_2: $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$; $\omega \mapsto \omega$

f_3: $\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$; $\omega \mapsto \omega$

f_4: $\sqrt[3]{2} \mapsto \sqrt[3]{2}$; $\omega \mapsto \omega^2$

f_5: $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$; $\omega \mapsto \omega^2$

f_6: $\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$; $\omega \mapsto \omega^2$

For å sjekke om gruppen er abelsk, kan vi for eksempel sjekke om $f_2 \circ f_5 = f_5 \circ f_2$. Obs! Husk at: $\omega = e^{2\pi i/3}$, s.a. $\omega^3 = \left(e^{2\pi i/3}\right)^3 = e^{2\pi i} = 1$.

$$f_2 \circ f_5\left(\sqrt[3]{2}\right) = f_2\left(\omega\sqrt[3]{2}\right) = f_2(\omega)f_2\left(\sqrt[3]{2}\right) = \omega \cdot \omega\sqrt[3]{2} = \omega^2\sqrt[3]{2}$$
$$f_5 \circ f_2\left(\sqrt[3]{2}\right) = f_5\left(\omega\sqrt[3]{2}\right) = f_5(\omega)f_5\left(\sqrt[3]{2}\right) = \omega^2 \cdot \omega\sqrt[3]{2} = \sqrt[3]{2}$$

Dermed er $f_2 \circ f_5 \neq f_5 \circ f_2$, det vil si at den ikke er abelsk. Dette medfører at $Gal(L/\mathbb{Q}) \cong S_3$

5.4. Galoisteoriens fundamentalteorem

I den neste delen oppgaven skal vi se på Galois sitt fundamentalteorem. Denne beskriver forholdet mellom undergrupper og underkropper. Husk at man ikke kaller teoremer for fundamentalteoremer for ingen grunn. Se kapittel 7.3 side 161-166 i [6].

[10] $f_2\left(\omega\sqrt[3]{2}\right) = f_2(\omega)f_2\left(\sqrt[3]{2}\right)$ er homomorfiegenskapen.

Teorem 9a.*: (*Første del av Galois Fundamental teorem)

La $F \subset L$ være en Galois utvidelse.

- For en mellomliggende kropp $F \subset K \subset L$, så har dens Galois gruppe $Gal(L/K) \subset Gal(L/F)$ fikserte kropper $L_{Gal(L/K)} = K$. Videre, $|Gal(L/K)| = [L: K]$ og $[Gal(L/F): Gal(L/K)] = [K: F]$.
- For en undergruppe $H \subset Gal(L/F)$, dens fikserte kropp $F \subset L_H \subset L$ har Galoisgruppen $Gal(L/L_H) = H$. Videre $[L: L_H] = |H|$ og $[L_H : F] = [Gal(L/F) : H]$

Hva lærer vi av den første delen av fundamentalteoremet? Kort sagt, gitt en kroppsutvidelse L/F som er endelig og en Galois- utvidelse, så er det en en-til-en korrespondanse mellom dens mellomliggende kropper og undergrupper av dens Galoisgruppe. Altså for hver mellomliggende kropp K av L/F, så er den tilhørende undergruppen bare $Aut(L/K)$, det vil si mengden av de automorfiene i $Gal(L/F)$ som fikserer alle elementene i K. Teoremet forteller også at størrelsen på undergruppen er lik indeksen til kroppen inni L.

Teorem 9b.*: (*Andre del av Galois Fundamental teorem)

La $F \subset L$ være en Galois utvidelse. Da vil avbildningen mellom mellomliggende kropper $F \subset K \subset L$ og undergrupper $H \subset Gal(L/F)$ være gitt ved:

$$K \mapsto Gal(L/K)$$

$$H \mapsto L_H$$

Reverse inklusjoner, er inverse av hverandre. Videre, hvis en underkropp K korrosponderer til en undergruppe H under disse avbildningene, da er K Galois over F hvis, og bare hvis, H er normal i $Gal(L/F)$. Når dette skjer, da er det en naturlig isomorfi:

$$Gal(L/F)/H \simeq Gal(K/F)$$

Hva er det denne andre delen av fundamentalteoremet egentlig forteller oss? Teoremet forteller at hvis en undergruppe er normal, så vil dens tilhørende underkropp også være en normal utvidelse og omvendt. Det samme gjelder hvis en undergruppe ikke er normal, så vil dens korresponderende underkropp heller ikke være en normal utvidelse og omvendt. I tillegg, hvis undergruppen er normal, så vil det medføre en isomorfisme mellom $Gal(K/F)$ og faktorgruppen $Gal(L/F)/H$. Dette betyr at vi ikke bare vet at K/F er en Galois utvidelse, men vi vet også nøyaktig hva dens Galoisgruppe er!

.

I det neste eksempelet, så skal vi se på hvordan vi kan anvende Galois Fundamentalteorem.

Eksempel 2.5.: Finn alle underkropper av L og vis at de korresponderer til undergrupper av $Gal(L/\mathbb{Q})$

Lager en tabell over komposisjonene som følger[11]:

∘	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_3	f_1	f_6	f_4	f_5
f_3	f_3	f_1	f_2	f_5	f_6	f_4
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

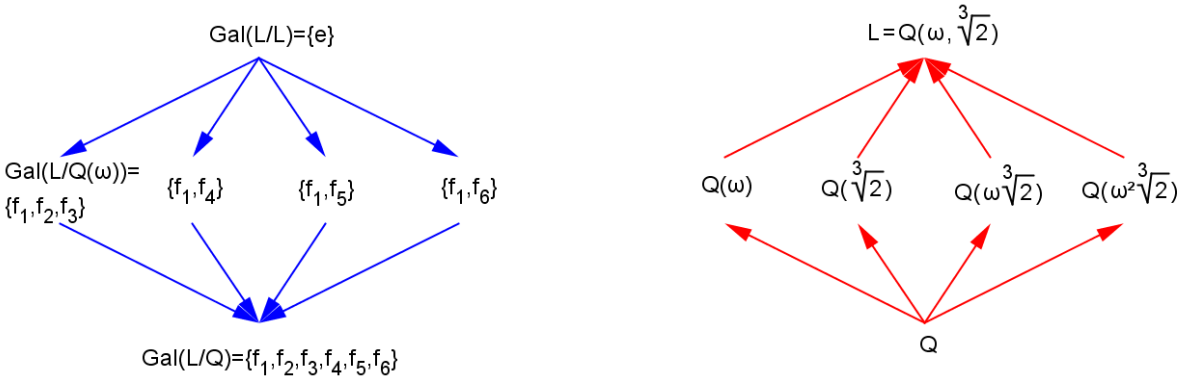
Tabell 1 komposisjonstabell

De seks undergruppene av G og deres tilhørende underkropper, er som beskrevet i fundamentalteoremet:

$$\{e\} = \{f_1\} \quad \leftrightarrow \quad L = \mathbb{Q}[\omega, \sqrt[3]{2}]$$
$$\{f_1\ , f_4\} \quad \leftrightarrow \quad \mathbb{Q}[\sqrt[3]{2}]$$
$$\{f_1, f_6\} \quad \leftrightarrow \quad \mathbb{Q}[\omega^2\sqrt[3]{2}]$$
$$\{f_1, f_5\} \quad \leftrightarrow \quad \mathbb{Q}[\omega\sqrt[3]{2}]$$
$$\{f_1, f_2, f_3\} \quad \leftrightarrow \quad \mathbb{Q}[\omega]$$
$$\{f_1, f_2, f_3, f_4, f_5, f_6\} \quad \leftrightarrow \quad \mathbb{Q}$$

Den trivielle undergruppen, (inneholder bare identitetselementet), korresponderer til hele L. $\{f_1\ , f_4\} \quad \leftrightarrow \quad \mathbb{Q}[\sqrt[3]{2}]$ ettersom f_4 fikserer eller holder $\sqrt[3]{2}$ fast, $\{f_1, f_6\} \quad \leftrightarrow \quad \mathbb{Q}[\omega^2\sqrt[3]{2}]$ siden f_6 fikserer $\omega^2\sqrt[3]{2}$, $\{f_1, f_5\} \quad \leftrightarrow \quad \mathbb{Q}[\omega\sqrt[3]{2}]$ fordi f_5 fikserer $\omega\sqrt[3]{2}$ og til slutt $\{f_1, f_2, f_3\} \quad \leftrightarrow \quad \mathbb{Q}[\omega]$ på grunn av f_2, f_3 fikserer ω. Hele gruppen G svarer til den nederst liggende kroppen $\mathbb{Q}$.

[11] Se tillegget for en interessant sammenligning mellom automorfiene i denne kroppen og automorfiene til en likesidet trekant.



Figur 16 Avbildninger av undergruppene av Gal(L/Q) og de tilhørende underkroppene av L

Legg merke til at pilene går fra minst mot størst (reverse inklusjoner er inverse av hverandre)

$$K_1 \subset K_2 \subset L \Rightarrow Gal(L/K_1) \supset Gal(L/K_2)$$

Vi kan se at de to figurene samstemmer ved å betrakte følgende, (som er et resultat fra første del av fundamentalteoremet):

$$|Gal(L/\mathbb{Q}(\omega)| = [L:\mathbb{Q}(\omega)] = \left[\mathbb{Q}\left(\omega, \sqrt[3]{2}\right): \mathbb{Q}(\omega)\right] = \frac{\left[\mathbb{Q}\left(\omega, \sqrt[3]{2}\right): \mathbb{Q}\right]}{[\mathbb{Q}(\omega): \mathbb{Q}]} = \frac{6}{2} = 3$$

$|Gal(L/\mathbb{Q}(\omega)| = 3$ stemmer jo, ettersom undergruppen som kjent består av de tre elementene $\{f_1, f_2, f_3\}$.

$$\left|Gal(L/\mathbb{Q}(\sqrt[3]{2})\right| = \left[L:\mathbb{Q}(\sqrt[3]{2})\right] = \left[\mathbb{Q}\left(\omega, \sqrt[3]{2}\right): \mathbb{Q}(\sqrt[3]{2})\right] = \frac{\left[\mathbb{Q}\left(\omega, \sqrt[3]{2}\right): \mathbb{Q}\right]}{\left[\mathbb{Q}\left(\sqrt[3]{2}\right): \mathbb{Q}\right]} = \frac{6}{3} = 2$$

$\left|Gal(L/\mathbb{Q}(\sqrt[3]{2})\right| = 2$, som stemmer med at undergruppen består av elementene $\{f_1, f_4\}$.

Fundamentalteoremet sier også noe om kroppsutvidelsene og undergruppene er normale eller ikke. Vi vet jo at utvidelsen $\mathbb{Q}[\sqrt[3]{2}]$ ikke er normal (***Eksempel 2.1.***). Da vil den tilhørende undergruppen $\{f_1, f_4\}$ heller ikke være normal, ifølge teoremet. Men hva med $\mathbb{Q}[\omega^2\sqrt[3]{2}]$? Er denne utvidelsen normal? Det er kanskje ikke så lett å se, men da kan vi bare sjekke om dens tilhørende undergruppe $\{f_1, f_6\}$ er normal.

Vi vil sjekke om $f_i\{f_1, f_6\}f_i^{-1} = \{f_1, f_6\}, for\ alle\ i, der\ i \in [1,6]$[12].

$$f_1\{f_1, f_6\}f_1^{-1} = f_1\{f_1, f_6\}f_1 = f_1\{f_1, f_6\} = \{f_1, f_6\}$$
$$f_2\{f_1, f_6\}f_2^{-1} = f_2\{f_1, f_6\}f_3 = f_2\{f_3, f_4\} = \{f_1, f_5\} \neq \{f_1, f_6\}$$

Undergruppen $\{f_1, f_6\}$ er ikke normal, da kan heller ikke dens tilhørende underkropp $\mathbb{Q}[\omega^2\sqrt[3]{2}]$ være en normal utvidelse! Hva med $\mathbb{Q}(\omega)$? Er dette en normal utvidelse? Igjen ser vi på undergruppen for å svare på det.

$$f_1\{f_1, f_2, f_3\}f_1^{-1} = f_1\{f_1, f_2, f_3\}f_1 = f_1\{f_1, f_2, f_3\} = \{f_1, f_2, f_3\}$$
$$f_2\{f_1, f_2, f_3\}f_2^{-1} = f_2\{f_1, f_2, f_3\}f_3 = f_2\{f_3, f_1, f_2\} = \{f_1, f_2, f_3\}$$
$$f_3\{f_1, f_2, f_3\}f_3^{-1} = f_3\{f_1, f_2, f_3\}f_2 = f_3\{f_2, f_3, f_1\} = \{f_1, f_2, f_3\}$$
$$f_4\{f_1, f_2, f_3\}f_4^{-1} = f_4\{f_1, f_2, f_3\}f_4 = f_4\{f_4, f_5, f_6\} = \{f_1, f_3, f_2\}$$
$$f_5\{f_1, f_2, f_3\}f_5^{-1} = f_5\{f_1, f_2, f_3\}f_5 = f_5\{f_5, f_6, f_4\} = \{f_1, f_3, f_2\}$$
$$f_6\{f_1, f_2, f_3\}f_6^{-1} = f_6\{f_1, f_2, f_3\}f_6 = f_6\{f_6, f_4, f_5\} = \{f_1, f_3, f_2\}$$

Ettersom $f_i\{f_1, f_2, f_3\}f_i^{-1} = \{f_1, f_2, f_3\}, for\ alle\ i, der\ i \in [1,6]$, så betyr det at undergruppen er normal og dermed også at $\mathbb{Q}(\omega)$ er en normal utvidelse.

5.5. Referanser og valg av referanser

Jeg vil på det varmeste anbefale David A.Cox når det gjelder hans behandling av Galoisteorien! I hans bok finner man en mengde eksempler og oppgaver som virkelig kan hjelpe ens forståelse. Siden hele boken er dedikert til Galoisteorien, så kommer boken med en veldig grundig drøftelse av teamet. I Cox sin bok står også bevisene til resultatene i dette kapittelet. En kan også finne mye fint stoff om Galoisteorien på *Wikipedia*.

(1) *Famous Mathematics Quotes*:

http://www.math.okstate.edu/~wli/teach/fmq.html

(6) Cox, D.A. (2004). *Galois Theory.* New Jersey: Wiley.

(7) Fraleigh, J.B. (2003). *A First Course In Abstract Algebra.* Rhode Island:

Pearson Education

[12] Se ***Teorem 12*** i tillegget.

6. Origami

"It is not the business of a Mathematician to show that a straight line or circle can be drawn, but he tells you what he means by these; and if you understand him, you may proceed further with him; and it would not be to the purpose to object that there is no such thing in nature as a true straight line or perfect circle, for this is none of his concern: he is not inquiring how things are in matter of fact, but supposing things to be in a certain way, what are the consequences to be deduced from them; and all that is to be demanded from him is, that his suppositions be intelligible, and his inferences just from the suppositions he makes."

Anonymous (1736?)

Origami (*ori* som betyr "bretting" og *gami* betyr "papir"), er navnet på den japanske kunsten for papirbretting. Målet i denne kunsten er å forandre papir om til figurer uten bruk av lim eller å kutte i papiret. Moderne origamikonstruksjoner har vist at det er mulig å lage både utrolig komplekse og vakre figurer bare ved hjelp av bretting av et enkelt ark. En mener at kunsten begynte i det 17 århundre e.v.t. og ble populært i midten av 1900- årene.

Etter hvert ble matematikere og vitenskapsfolk også interessert i origami. De begynte å stille spørsmål som: Hva er mulig å gjøre med origami? Hvordan kan man brette et gitt objekt? Vitenskapsfolk stiller selvfølgelig ikke bare spørsmål, de leter også etter svar. De har blant annet funnet ut at enkelte problemer som er umulig med lovlig bruk av passer og linjal, faktisk lar seg løse ved origami – deriblant to av de klassiske problemene. Se [6] kapittel 10.3 side 273.

Bilde 10 I denne origami komposisjon, "Hummingbird and Trumpet Vine", så ble hvert blad, blomst og fuglen brettet fra et enkelt kvadratisk stykke papir, uten å kutte i arket.

6.1. Punkter vi kan konstruere med origami

Origamikonstruksjoner består bare av en rekke brettinger av et papir. Når du bretter et ark og deretter strekker arket ut igjen, så vil du se en linje på papiret. Det er disse linjene vi jobber med i origami-konstruksjoner. Ett nytt punkt er definert som snittet av to linjer.

Når vi skulle arbeide teoretisk med passer og linjal, så lagde vi en del aksiomer for å hjelpe oss. Det samme kan vi gjøre når vi skal arbeide med origami. Aksiomene for konstruksjoner med passer og linjal viser seg å være helt de samme som for konstruksjoner med origami. Eneste forskjellen er at vi med origamikonstruksjoner kan legge til et ekstra aksiom. Følgende resultat og flere av eksemplene og resultatene i dette kapittelet kan finnes i [6] kapittel 10.3 sidene 274-279.

K 3. Hvis punktene $\alpha_1 \neq \alpha_2$ ikke ligger på linjene $l_1 \neq l_2$, så kan vi tegne en linje l som reflekterer α_1 til et punkt på l_1 og α_2 til et punkt på l_2.

Vi danner altså sirkler og linjer med aksiomene K 1, K 2 og K 3, mens vi får punktene ved P 1, P 2 og P 3. Origamitall kan defineres som følger:

Definisjon 8.: Et komplekst tall α er et origamitall hvis det er en endelig sekvens som begynner med 0 og 1 og ender med α, der konstruksjonen er laget av aksiomene K 1, K 2, K 3, P 1, P 2 og P 3.

Det er mulig å vise at alle disse aksiomene kan gjøres utelukkende ved origami[13]. Istedenfor å bruke aksiomene i ***Definisjon 8.***, så skal vi bruke noen ekvivalente aksiomer som gjør det lettere for oss når vi skal arbeide med origami. Følgende aksiomer er kjent som Huzitas sine aksiomer, se [8] kapittel 1.2 side 2.

O 1. Gitt punktene p_1 og p_2, så kan vi brette en linje som går igjennom begge punktene.

O 2. Gitt punktene p_1 og p_2, så kan vi brette punktet p_1 på punktet p_2 (Da finner vi midtnormalen til linjesegmentet $\overline{p_1 p_2}$).

O 3. Gitt to linjer l_1 og l_2, så kan vi brette linjen l_1 på linjen l_2 (Da finner vi linjen som halverer vinkelen mellom linjene l_1 og l_2).

O 4. Gitt et punkt p og en linje l, så kan vi brette en normal på linjen l gjennom punktet p.

O 5. Gitt to punkter p_1, p_2 og en linje l, vi kan brette p_1 på linjen l, slik at brettingen lager en linje som går gjennom p_2.

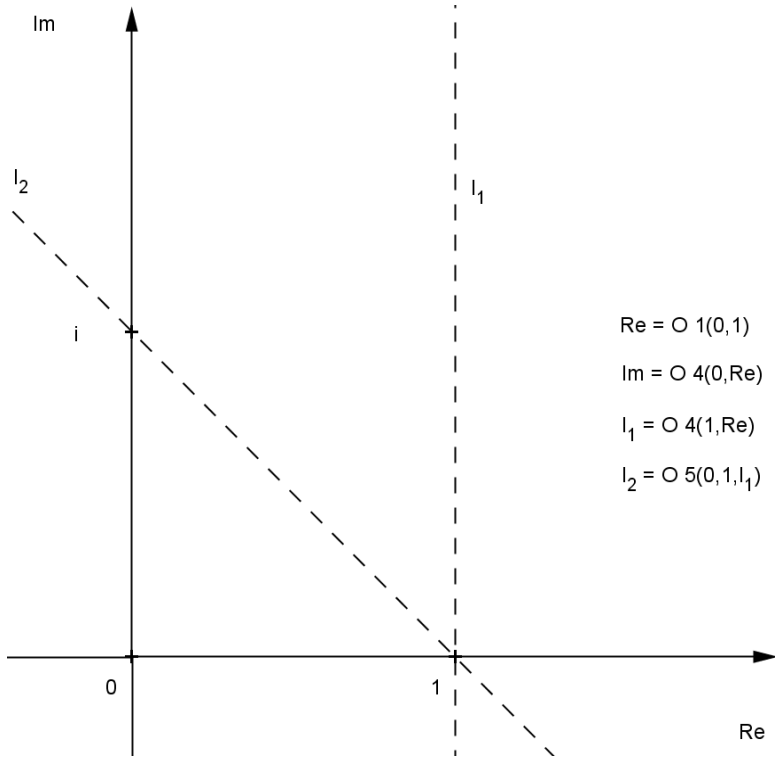
[13] Se kapittel 10 i [9].

O 6. Gitt to punkter p_1, p_2 og to linjer l_1, l_2, vi kan folde p_1 på l_1 og p_2 på l_2 med en enkel linje (Dette aksiomet er det samme som K 3).

For å gjøre skrivingen litt mer ryddig gjør vi som i artikkelen [8], der en tenker på hvert aksiom som en funksjon som tar punkter og linjer som input og gir en ny linje som output. I tillegg tillater ikke reglene i spillet å gjøre flere bretteopersasjoner på én gang. En må altså brette eller strekke arket ut igjen etter at en har anvendt et av aksiomene – se kapittel 10 side 149 i [9].

I vårt arbeid med passer og linjal begynte vi med å vise hvilke tallsystemer vi kunne konstruere. På samme måte kan vi vise at en kan konstruere de gaussiske heltallene bare ved hjelp av origami.

Eksempel 3.: Arket lar vi være det komplekse planet.



Figur 17 Konstruksjon av de gaussiske heltallene

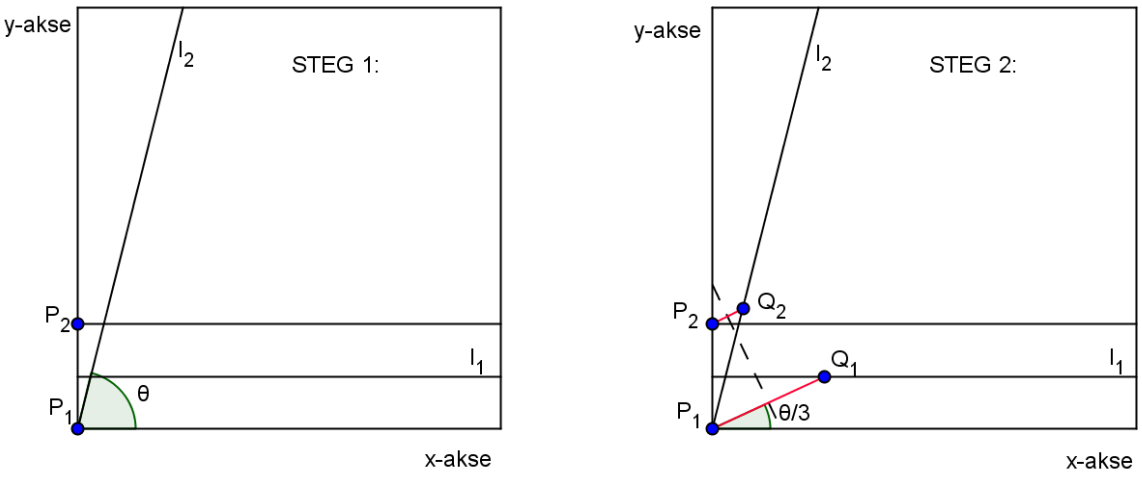
Begynner med å brette en linje gjennom punktene 0 og 1. Denne linjen lar vi være den reelle aksen. Bretter så en normal på den reelle aksen gjennom punktet 0. La den nye linjen være den imaginære aksen. For å danne punkter på den komplekse aksen, begynner vi med å brette linjen l_1 som er normalen på den reelle aksen gjennom punktet 1. Til slutt bretter vi en linje l_2, ved å ta punktet 0 til linjen l_1 slik at brettingen danner en linje gjennom punktet 1.

Skjæringen $Im \cap l_2$ gir vårt nye punkt i. Hvordan ville du ha brettet resten av de gaussiske heltallene?

Mange ble overrasket da de hørte at det var mulig å løse problemet med vinkelens tredeling ved hjelp av origami. Redaktørene i tidskriftet "*The American Mathematical Monthly*" ble også overrasket. I 1996 ble det skrevet en artikkel der det ble "bevist" at vinkelens tredeling er umulig med origami. Seks måneder senerer korrigerte de imidlertid dette og la til at en løsning på problemet allerede var blitt publisert over 20 år tidligere. Se artikkelen [10] til Robert J. Lang.

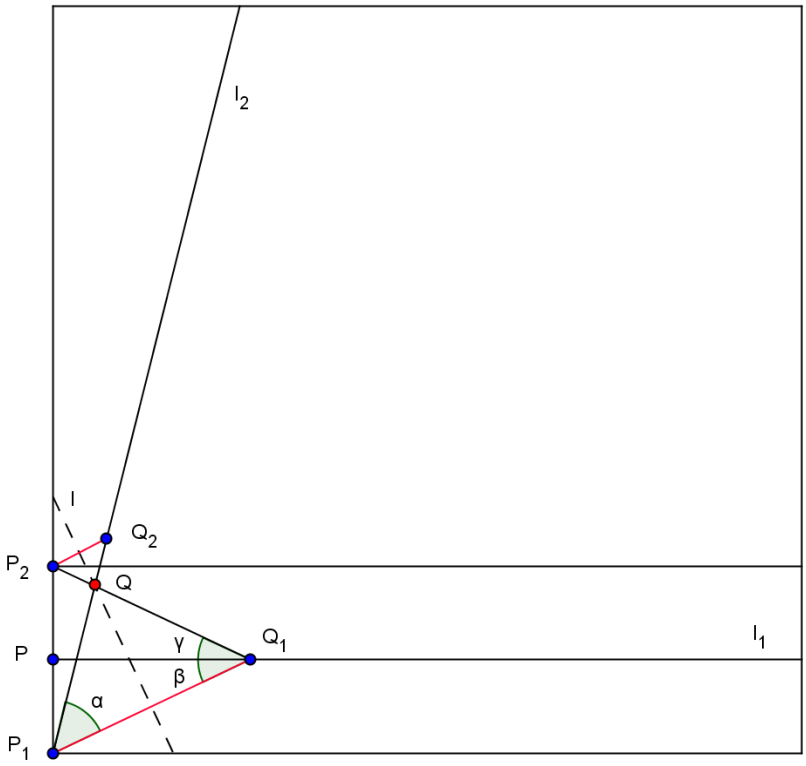
Vinkelens tredeling.: I figuren under er det vist i to steg hvordan en kan tredele en vilkårlig vinkel θ mellom $^{\pi}/_{4}$ og $^{\pi}/_{2}$. La bunnen på arket være vår $x-akse$ og ene siden på arket $y-aksen$, slik at P_1ligger i origo. Gitt en linje l_2 mellom $^{\pi}/_{4}$ og $^{\pi}/_{2}$ gjennom punktet P_1. Velger et punkt P_2 på $y-aksen$. Bretter en linje gjennom P_2 som er parallell med $x-aksen$, O 4$(P_2, y-akse)$. Så bretter vi linjen l_1 som er parallell og har lik avstand fra $x-aksen$ og normalen gjennom P_2 ved aksiom O 3.

I det andre steget skal vi brettet arket slik at vi flytter punktet P_1til linjen l_1 og P_2 til l_2 (O6(P_1, P_2, l_1, l_2)). Markerer punktene som muliggjør denne brettingen og kaller dem Q_1og Q_2 (Hvordan ville du ha funnet punktene $Q_1\ og\ Q_2$ kan ved origami?). Poenget er at disse punktene er speilinger av punktene P_1 og P_2 om den stiplete linjen. Det viser seg at vinkelen mellom $x-aksen$ og linjen $\overline{P_1Q_1}$ er $^{\theta}/_{3}$.



Figur 18 Vinkelens tredeling ved hjelp av origami

Bevis: Nå skal vi bevise at vinkelen mellom bunnen på papiret og linjen $\overline{P_1Q_1}$ virkelig er $\theta/3$.



Figur 19 Bevis av vinkelens tredeling

Vi tar utgangspunkt i figuren over. Først lar vi Q være skjæringspunktet mellom $\overline{P_1Q_2}$ og $\overline{P_2Q_1}$. Nå vil vi vise at Q ligger på den stiplete linjen. Vi vet at Q må ligge på linjen $\overline{P_1Q_2}$ og på linjen $\overline{P_2Q_1}$. Hvis vi nå speiler $\overline{P_1Q_2}$ om den stiplete linjen så får vi $\overline{P_2Q_1}$ og omvendt. Da ser vi at Q vil ligge på det samme punktet før og etter speiling. Dette er kun mulig hvis Q ligger på speilingslinjen. Q må altså ligge på l.

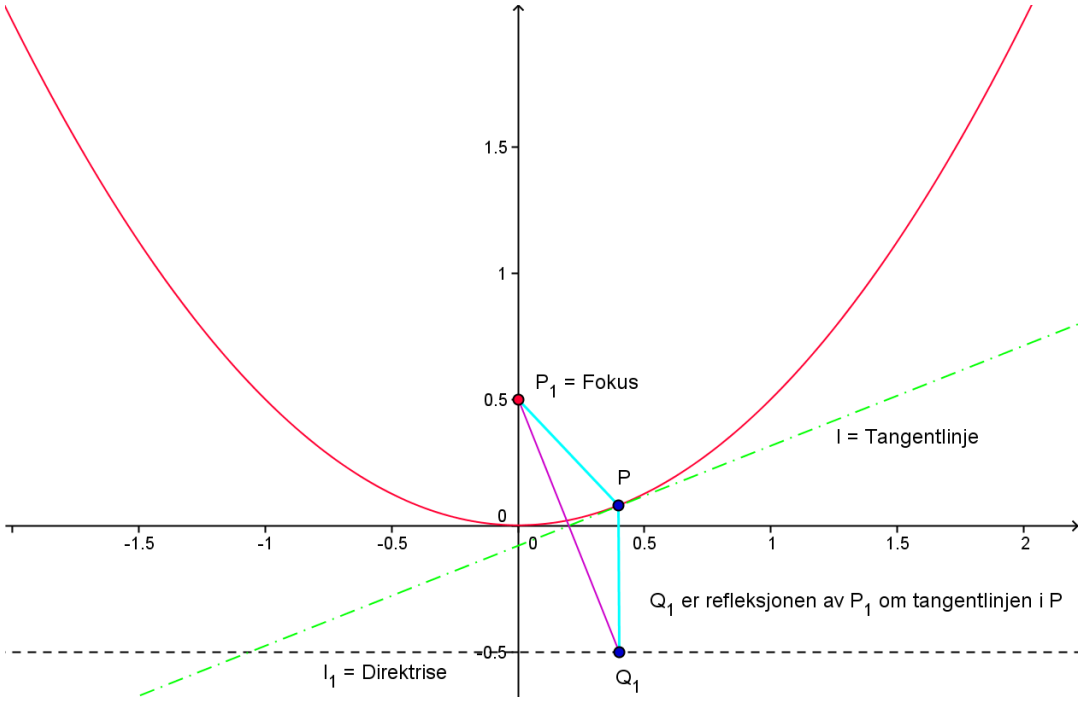
Neste steg er å vise at vinkelen θ (se ***Figur 18***) er lik vinklene $\alpha + \beta$. Fra trenkanten ΔPQ_1P_1, så ser vi at vinkelen mellom bunnen på arket og linjen $\overline{P_1Q_1}$ må være β. Dermed er $\theta = \alpha + \beta$. På samme måte kan vi ved hjelp av trekantene $\Delta\, P_1PQ_1$ og $\Delta\, P_2PQ_1$ se at $\beta = \gamma$. Ved trekanten ΔP_1QQ_1 ser vi at $\alpha = \beta + \gamma$ (ettersom linjen l står normalt på $\overline{P_1Q_1}$ og deler linjen i to like store deler). Til slutt:

$\theta = \alpha + \beta \Leftrightarrow (\beta + \gamma) + \beta \Leftrightarrow \theta = 3\beta \Leftrightarrow \beta = \theta/3$.■

Så langt har vi vist at det er mulig å tredele en vinkel mellom $\pi/4$ og $\pi/2$. Hva da med en vinkel som er utenfor dette intervallet? Alt vi trenger, er å kunne halvere og fordoble vinkler. Ser du hvordan en kan bruke dette for å tredele en vilkårlig vinkel?

6.2. Viktige resultater og bevis

Før vi går videre, vil vi gjerne analysere hva vi egentlig har gjort i origamikonstruksjonen over. Det viser seg at det hele dreier seg om simultantangenten til to parabler. Husk at parabler er definert ved at alle punktene på parabelen har samme avstand fra fokuset (eller brennpunktet) og normalt ned på direktrisen (eller styringslinjen).



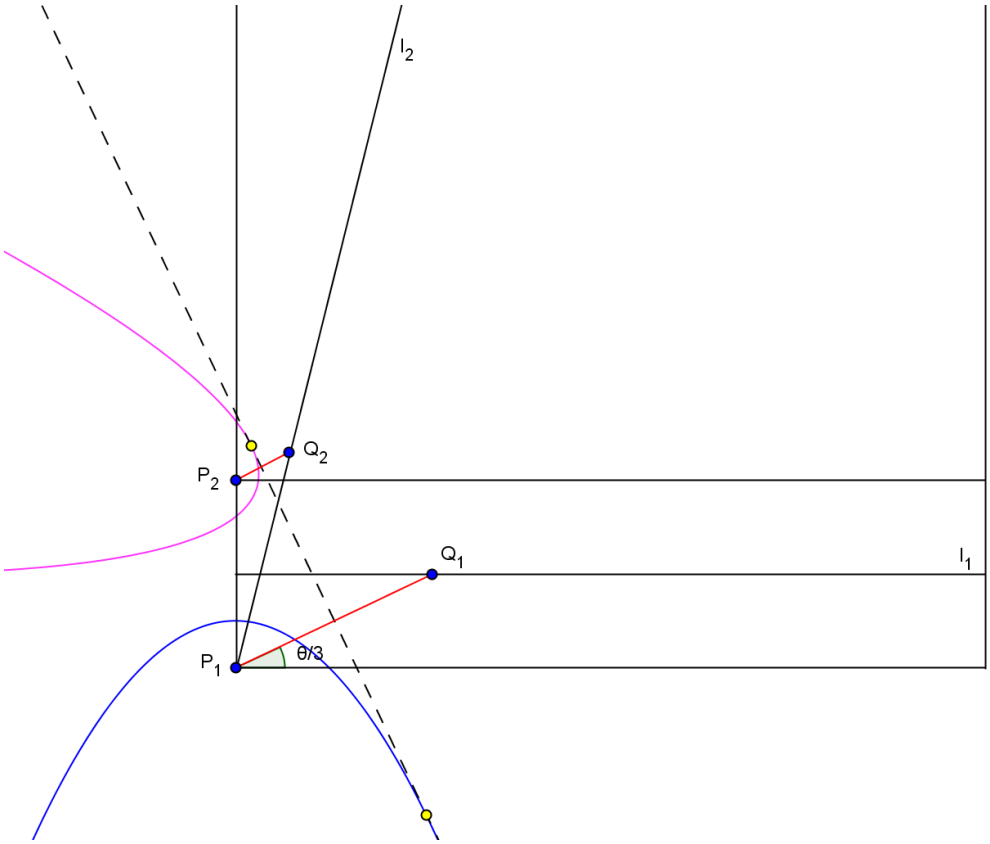
Figur 20 En parabel[14]

Lemma 4.: I planet, la P_1være et punkt som ikke ligger på en linje l_1. Gitt en annen linje l, så vil refleksjonen til punktet P_1om linjen l ligge på linjen l_1 hvis, og bare hvis, l er tangenten til en parabel med fokus P_1 og direktrise l_1.

Vi kan illustrere lemmaet ved igjen å se litt nærmere på ***Figur 18***. Brettingen foregikk ved at vi tok punktet P_1 til Q_1 og punktet P_2 til Q_2, der punktene Q_1 og Q_2 lå på linjene l_1 og l_2. Ettersom punktet

[14] Det er ofte vanlig å skrive en parabel på standard form. Det betyr at en skriver parabler på formen $x^2 = 4py$ eller $y = \frac{x^2}{4p}$, der parabelen har fokus $F(0,p)$ og direktrise $y = -p$. Dette er formen for parabler med bunnpunkt i origo. Hvis parabelen $y = x^2$ var forskjøvet slik: $y - (-1) = (x-2)^2$, så ville parabelen ha fokus i $(0+2, \left(\frac{1}{4}\right) - 1) = (2, -3/4)$ og direktrise $y - (-1) = -1/4 \Leftrightarrow y = -5/4$ se side 21 i [11].

Q_1 var refleksjonen til punktet P_1om den stiplete linjen, så betyr det at denne stiplete linjen er tangentlinjen til parabelen med fokus i P_1og direktrise l_1. Analogt vil den stiplete linjen også være tangentlinjen til parabelen med fokus i P_2 og direktrise l_2. Vi kan altså finne simultantangenten, (hvis en slik finnes), til to parabler ved hjelp av origami. Den underliggende geometrien som vi brukte i origamioperasjonene for å tredele en vinkel mellom $\pi/4$ og $\pi/2$, er avbildet i neste figur.



Figur 21 Den underliggende geometrien i tredelingen av vinkelen θ

Den stiplete linjen i ***Figur 21*** er et eksempel på K 3. I det neste eksempelet skal vi se hvordan vi kan bruke dette.

Eksempel 4.: Vi skal nå løse den kubiske ligningen $x^3 + ax + b = 0$[15], bare ved bruk av simultantangenten til to bestemte parabler. Bruker eksempelet gitt i kapittel 10.3, side 275 i Cox sin bok [6]. Her er $a, b \in \mathbb{R}$ og $b \neq 0$ og parablene er gitt ved:

[15] Dette er faktisk det samme som en generell tredjegradsligning $ax^3 + bx^2 + cx + d = 0$. En kan vise at det alltid er mulig å kvitte seg med leddet x^{n-1} (ved hjelp av substitusjon) fra et polynom av grad n. Poenget er at vi kan løse alle tredjegradspolynomer med origami!

$$\left(y-\frac{1}{2}a\right)^2 = 2bx \quad og \quad y=\frac{1}{2}x^2$$

Lar l være simultantangenten med stigningstall m til disse to parablene i punktene (x_1, y_1) og (x_2, y_2). Tangentlinjen vil være definert ved $y = mx + z$ (ettersom vi vet at denne ikke er vertikal), hvor m er en løsning til vår kubiske ligning. Direktrisene som vi trenger for å brette simultantangenten er gitt ved $D_1: x = -\frac{b}{2}$ (se fotnote 14) og $D_2: y = -\frac{1}{2}$.

Først vil vi finne stigningstallet til tangentlinjen i punktet (x_1, y_1), altså stigningen til tangenten i den første parabelen. For å finne dette stigningstallet kan vi derivere den første ligningen implisitt med hensyn på x (vi behandler y som en funksjon av x):

$$\frac{d}{dx}\left(y-\frac{1}{2}a\right)^2 = \frac{d}{dx}2bx \Leftrightarrow 2\left(y-\frac{1}{2}a\right)\frac{dy}{dx} = 2b \Leftrightarrow \frac{dy}{dx} = \frac{b}{y-\frac{1}{2}a}$$

Dermed så vet vi at stigningstallet m i punktet (x_1, y_1) må være $m = \frac{b}{y_1-\frac{1}{2}a}$. m må altså være ulik null og $y_1 - \frac{1}{2}a = \frac{b}{m}$. Fra dette, så ser vi at:

$$x_1 = \frac{\left(y_1-\frac{1}{2}a\right)^2}{2b} = \frac{\left(\frac{b}{m}\right)^2}{2b} = \frac{b}{2m^2}$$
$$y_1 = \frac{b}{m} + \frac{a}{2}$$

Gjenta, men nå med stigningstallet til tangentlinjen til den andre parabelen i punktet (x_2, y_2). Da finner vi:

$$x_2 = m \quad og \quad y_2 = \frac{m^2}{2}$$

Videre kan vi substituere inn disse verdiene:

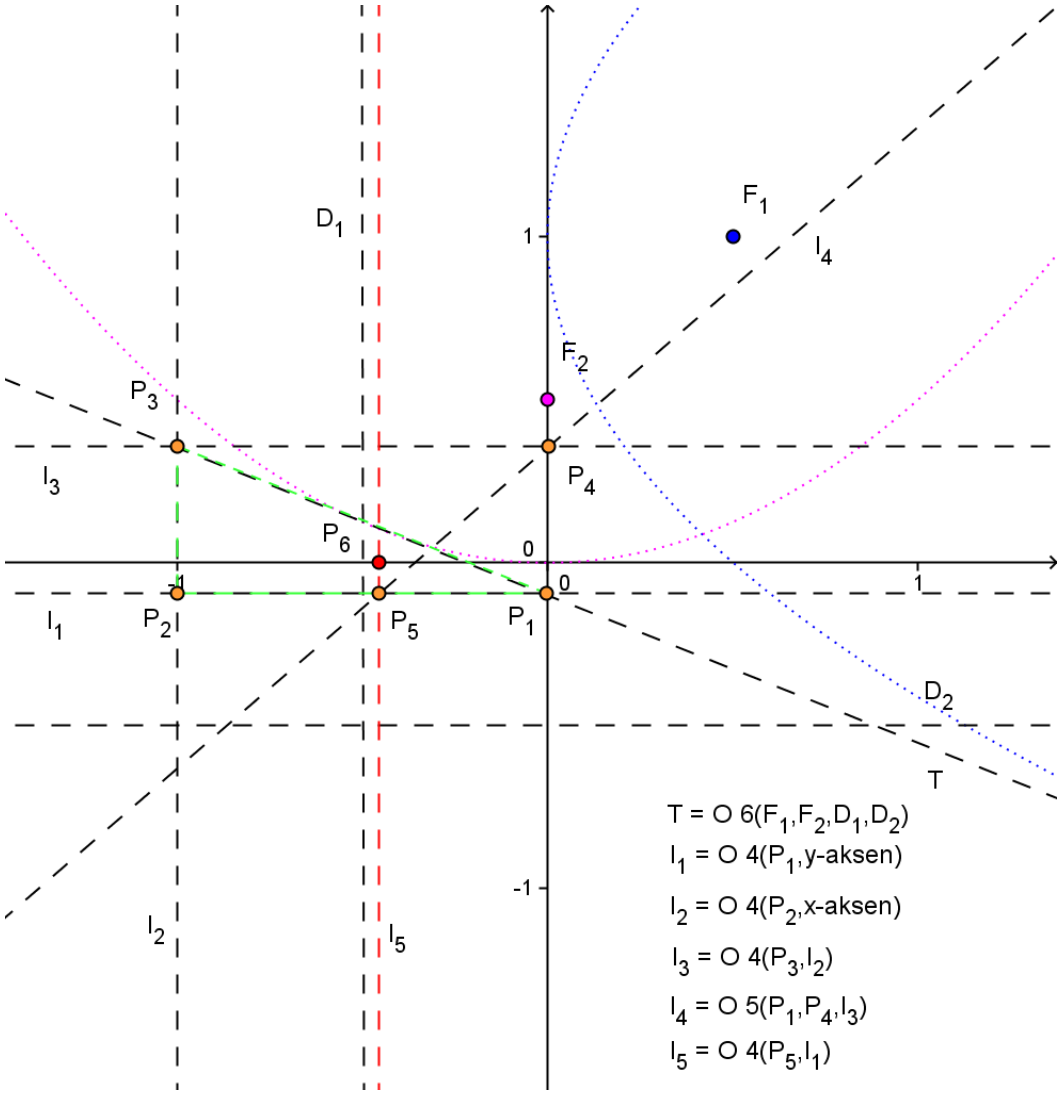
$$m = \frac{y_2-y_1}{x_2-x_1} = \frac{\frac{m^2}{2}-\left(\frac{b}{m}+\frac{a}{2}\right)}{m-\frac{b}{2m^2}} = \frac{m^4-2bm-am^2}{2m^3-b}$$

Ettersom $m \neq 0$, så følger det at m tilfredstiller ligningen:

$$m^3 + am + b = 0$$

Dermed er stigningstallene til simultantangentene til parablene røtter av den kubiske ligningen $m^3 + am + b = 0$.

Vi skal nå se på et spesielt tilfelle, nemlig når $a = 2$ og $b = 1$. Nå skal vi finne en løsning til ligningen $x^3 + 2x + 1$ bare ved hjelp av bretting. For å gjøre dette må vi finne stigningstallet m til simultantangenten til de overnevnte parablene, der $(,0)$ er en løsning på ligningen. Det kan vises ved at den første parabelen har fokus $F_1 = (\frac{1}{2}, 1)$ og direktrise $D_1: x = -\frac{1}{2}$ og at den andre parabelen har fokus $F_2 = (0, \frac{1}{2})$ og direktrise $D_2: y = -\frac{1}{2}$. Brettingen er gitt i figuren under.

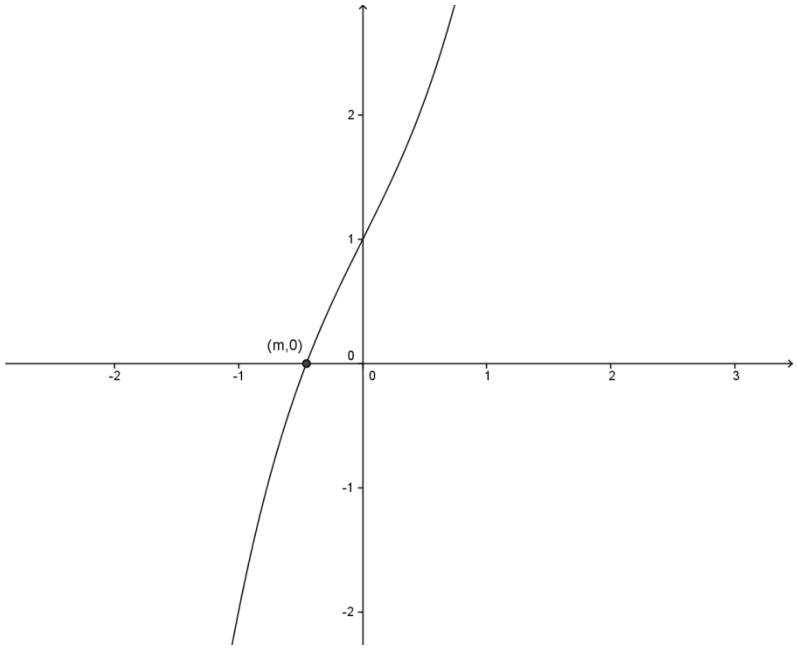


Figur 22 En løsning av ligningen $x^3 + 2x + 1$ ved papirbretteting

Vi begynner med et koordinatsystem, som vi allerede har vist kan brettes. Bretter direktrisene D_1 og D_2 og merker punktene F_1 og F_2. Deretter bretter vi simultantangenten T, ved å brette brennpunktene F_1 og F_2 til direktrisene D_1 og D_2. Skjæringspunktet mellom $y - aksen$ og simultantangenten kaller vi for P_1. Oppreiser normalen l_1 på $y - aksen$ gjennom punktet P_1. Videre nedfeller vi en normal l_2 på $x - aksen$ gjennom $(-1,0)$ og kaller snittene mellom l_2 og l_1 for P_2 og snittet mellom T og l_2 for P_3. Nå ser vi at absoluttverdien av avstanden mellom P_2 og P_3 faktisk er lik m.

Da gjenstår det bare å finne punktet $(,0)$. Husk at dette vil være et nullpunkt ettersom m tilfredstiller ligningen $m^3 + 2m + 1 = 0$. En kan finne fortegnet til m ved for eksempel å løse tredjegradsligningen. I dette tilfellet vil ligningen ha to komplekse røtter og en negativ reell rot. Bretter igjen en

normal som vi kaller l_3 på l_2 gjennom P_3. Skjæringen mellom $y-aksen$ og l_3 kaller vi for P_4. Deretter bretter vi en linje l_4, ved å ta P_1 opp til linjen l_3, slik at brettingen danner en linje gjennom punktet P_4. Skjæringen mellom l_4 og l_1 gir punktet P_5. Til slutt bretter vi normalen l_5 på l_1 gjennom P_5. Snittet mellom l_5 og $x-aksen$ gir punktet P_6, som nettopp er punktet $(,0)$. Vi har følgelig løst et tredjegradspolynom bare ved hjelp av brettinger!



Figur 23 Nullpunkt til polynomet m^3+2m+1

Mengden av origamitall har følgende struktur. Teoremet vil trolig virke meget kjent. Det eneste "nye" i forhold til rene passer- og linjalkonstruksjoner, er at vi nå kan konstruere eller brette kubikkrøtter.

Teorem 10.: Mengden $\mathcal{O}=\{\alpha\in\mathbb{C}|\alpha\ er\ et\ origamitall\}$ er en underkropp av $\mathbb{C}$. Dessuten vil:

a) La $\alpha=a+ib$, hvor $a,b\in\mathbb{R}$. Da er $\alpha\in\mathcal{O}$ hvis, og bare hvis, $a,b\in\mathcal{O}$.

b) $\alpha\in\mathcal{O}$ impliserer at $\sqrt{\alpha},\sqrt[3]{\alpha}\in\mathcal{O}$.

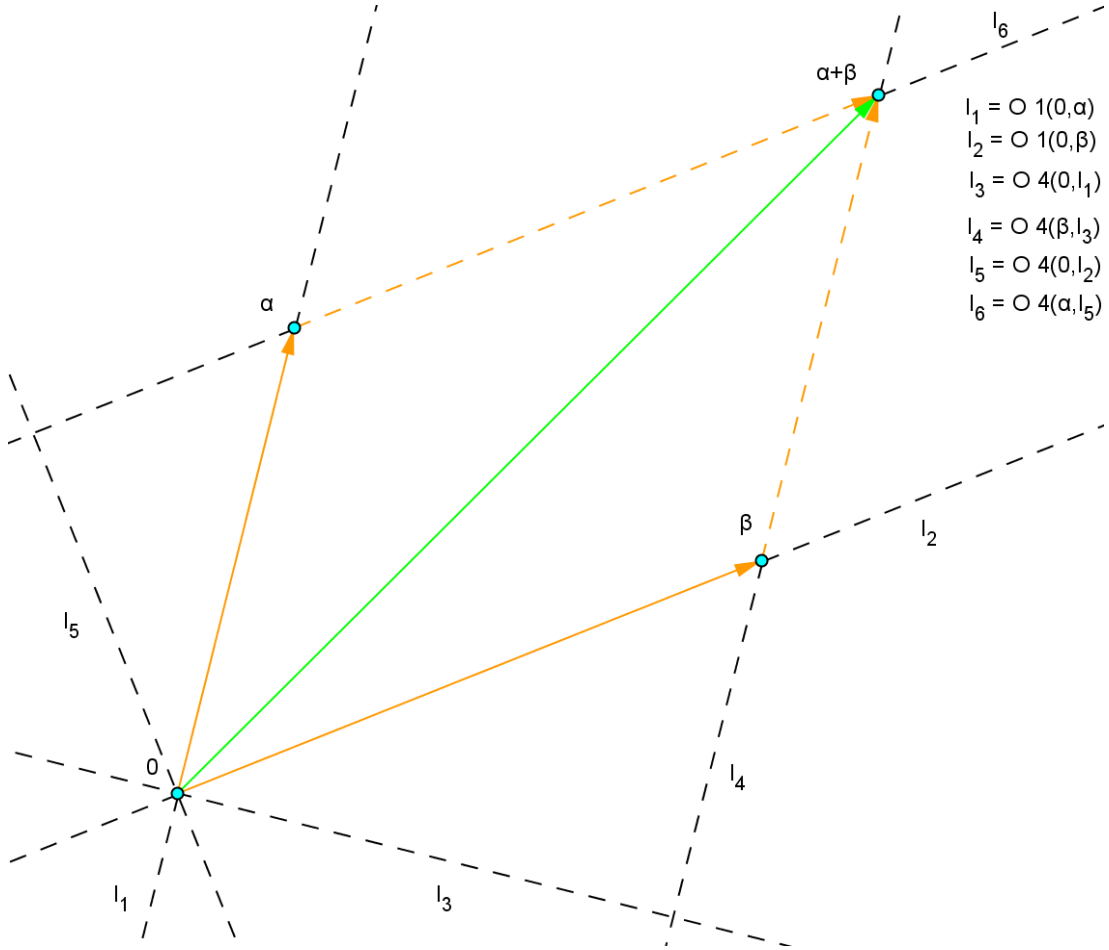
c) Et komplekst tall α ligger i $\mathcal{O}$ hvis, og bare hvis, det er underkropper

$$\mathbb{Q}=F_0\subset F_1\ldots\subset F_{n-1}\subset F_n\subset\mathbb{C}$$

slik at $\alpha\in F_n$og $[F_i:F_{i-1}]=2\ eller\ 3$ for $1\leq i\leq n$.

Bevis: Beviset er ganske likt bevisene vi gjorde i vårt tidligere arbeid. Interesserte må gjerne se kapittel 10.3 side 276 i [6]. Vi skal nøye oss med å bevise at origamitallene faktisk danner en kropp og vise at $\alpha\in\mathcal{O}\Rightarrow\sqrt[3]{\alpha}\in\mathcal{O}$. La oss begynne med å vise at origami-

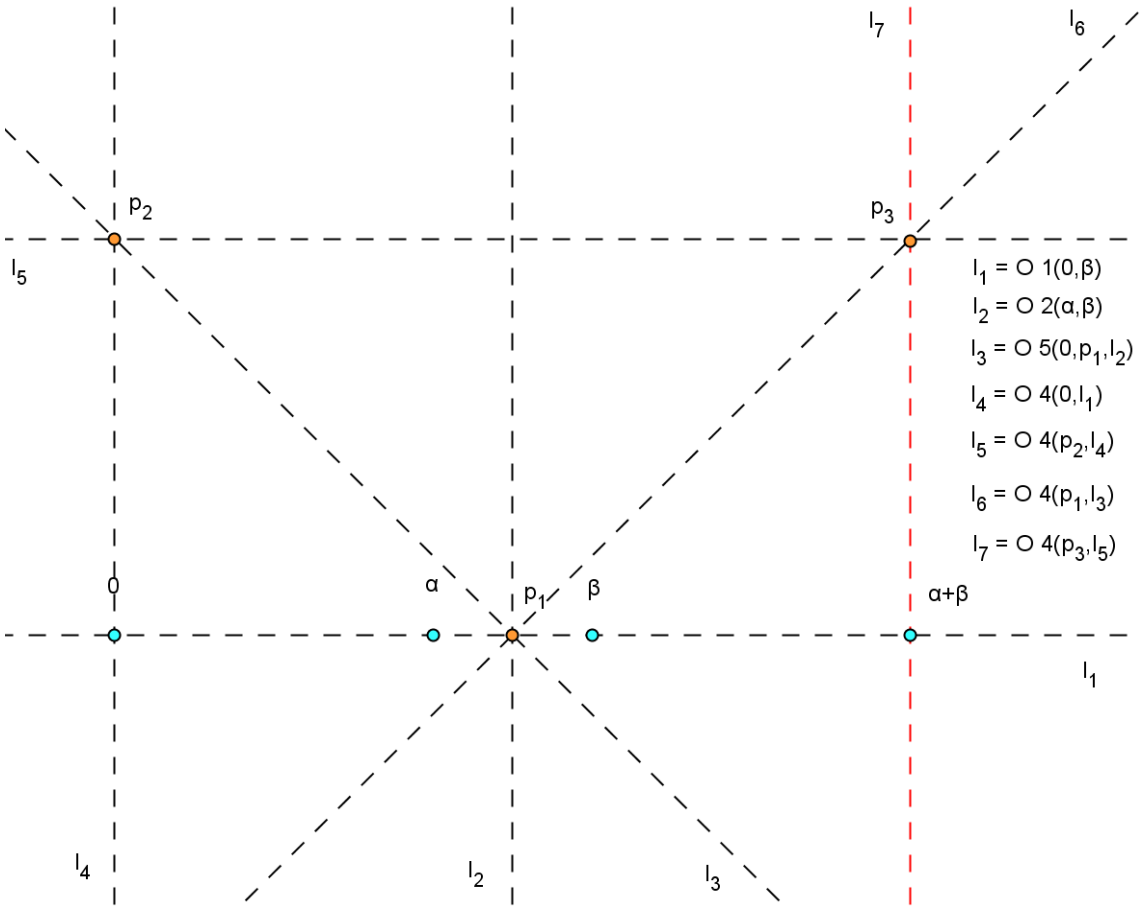
tallene er lukket under addisjon. Som i arbeidet med passer og linjal sjekker vi først tilfellet når vektorene ikke er parallelle.



Figur 24 Bretting når vektorene ikke er parallelle

Vi begynner med punktene $0, \alpha \; og \; \beta$ som er konstruerbare. Ønsket er å brette $\alpha + \beta$. Bretter linjen l_1 gjennom punktene $0 \; og \; \alpha$ og l_2 gjennom $0 \; og \; \beta$. Deretter bretter vi normalen l_3 på l_1 gjennom punktet 0. Bretter så normalen l_4 på l_3 gjennom β. Linjen l_5 er normalen på l_2 gjennom 0. Til slutt bretter vi normalen l_6 på l_5 gjennom α. Da er $\alpha + \beta = l_4 \cap l_6$.

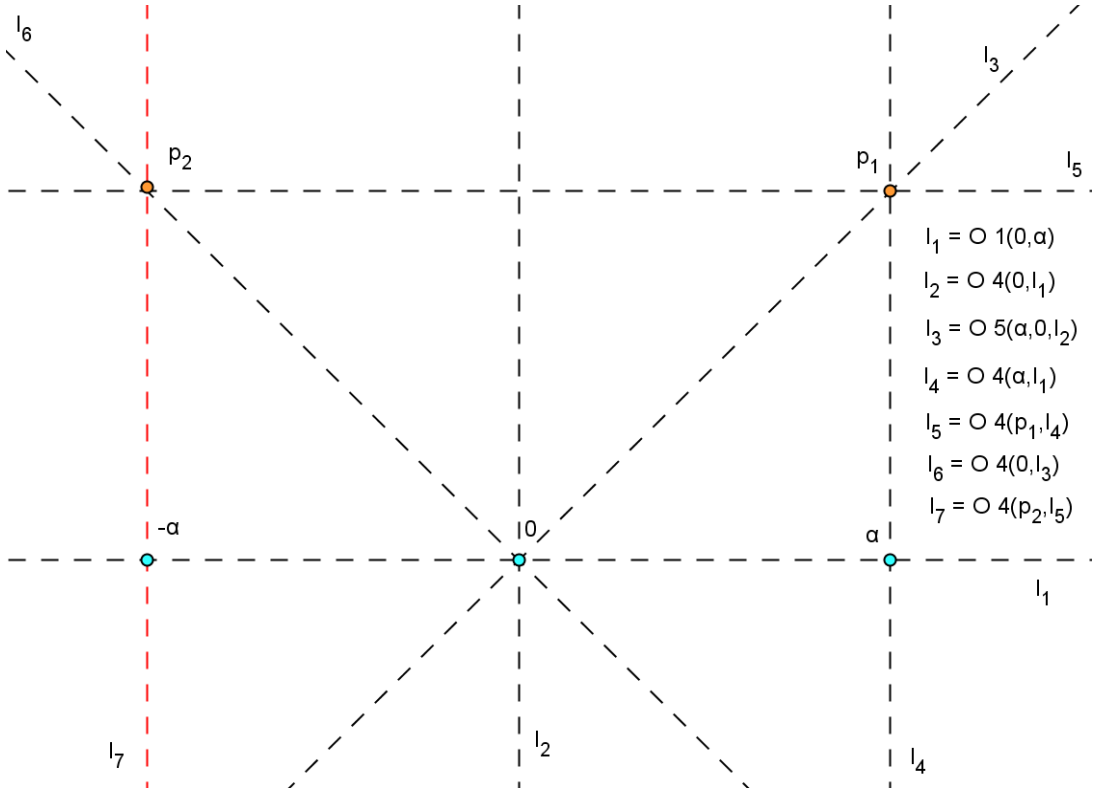
Når vektorene derimot er parallelle, så kan vi brette på denne måten:



Figur 25 Bretting når vektorene er parallelle

Først bretter vi linjen l_1 som går gjennom $0, \alpha \; og \; \beta$. Deretter bretter vi midtnormalen l_2 mellom punktene $\alpha \; og \; \beta$. Snittet mellom $l_1$og l_2 gir punktet p_1. Så bretter vi linjen l_3 ved å ta punktet 0 til linjen l_2, slik at det går en linje gjennom p_1. Videre bretter vi l_4, som er normalen på l_1, gjennom 0. Skjæringen mellom linjene l_3 og l_4 gir punktet p_2. Bretter deretter normalen l_5 på l_4 gjennom p_2. Nå bretter vi normalen l_6 på l_3 gjennom punktet p_1. Da vil $l_5 \cap l_6 = p_3$. Til slutt lager vi normalen l_7 på l_5 gjennom p_3. Det betyr at skjæringen mellom l_1 og l_7 gir det ønskede punktet $\alpha + \beta$.

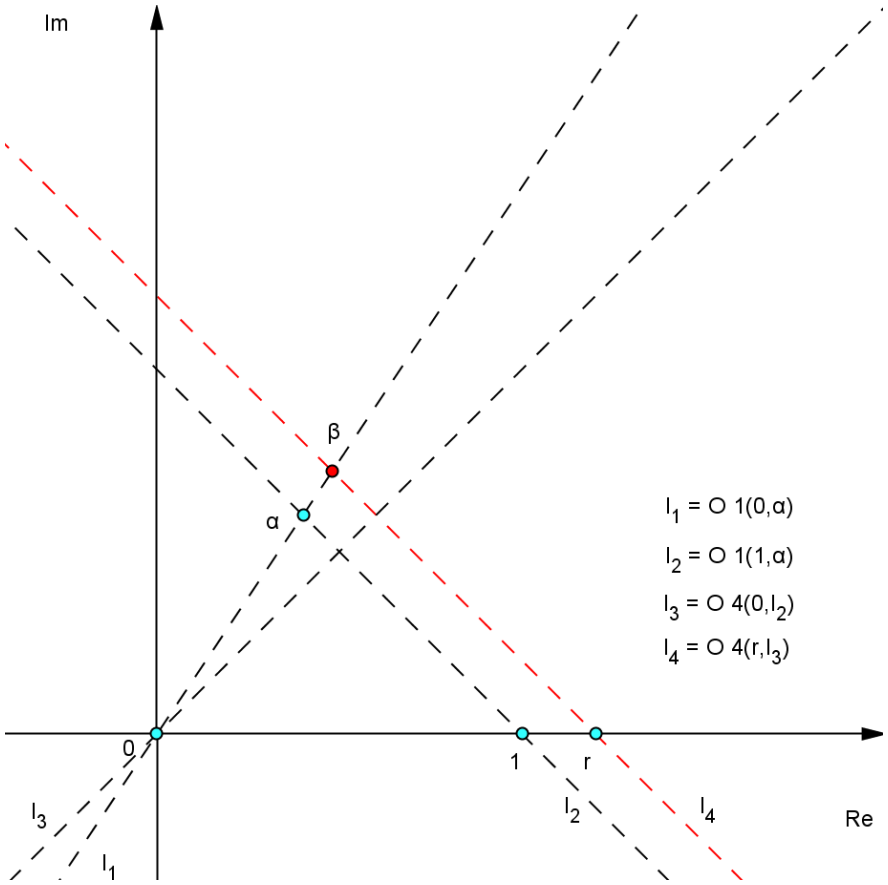
Og til slutt negative tall:



Figur 26 Additive inversen til α ved origami

Brettingen kan gjøres nesten helt likt som brettingen når α og β er parallelle, se figur. Dermed kan vi brette den additive inversen av et tall ved origami.

Origamitallene $\mathcal{O}$ er altså lukket under addisjon og subtraksjon. Nå skal vi vise at de også er lukket under multiplikasjon. Generelt er multiplikasjon av to komplekse tall gitt ved: $\alpha\beta = (a + ib)(c + id) = ac + i(ad + bc) - bd$. Ifølge ligningen må vi kunne addere, subtrahere og multiplisere med i og reelle tall. Vi har allerede vist at addisjon og subtraksjon av origamitall går fint. Det neste blir å vise at vi kan multiplisere med reelle og komplekse tall. Multiplikasjon med et reelt tall er gitt i figuren under.



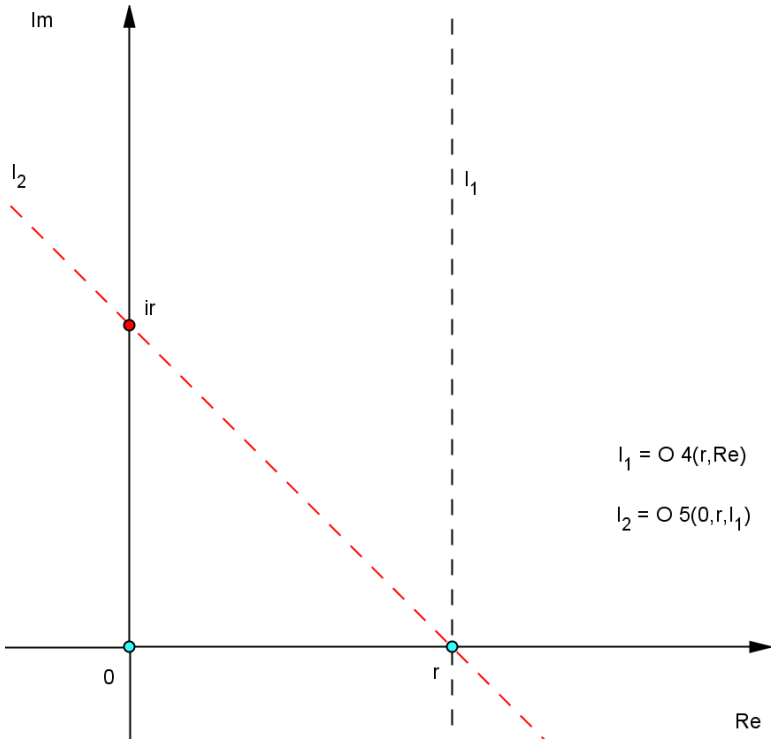
Figur 27 Multiplikasjon med et positivt reelt tall

Brettingene er som beskrevet i figuren. Poenget er at vi fra formlike trekanter får:

$$\frac{|\alpha|}{1} = \frac{|\beta|}{r} \Leftrightarrow |\beta| = r|\alpha|, \text{ der } r > 0$$

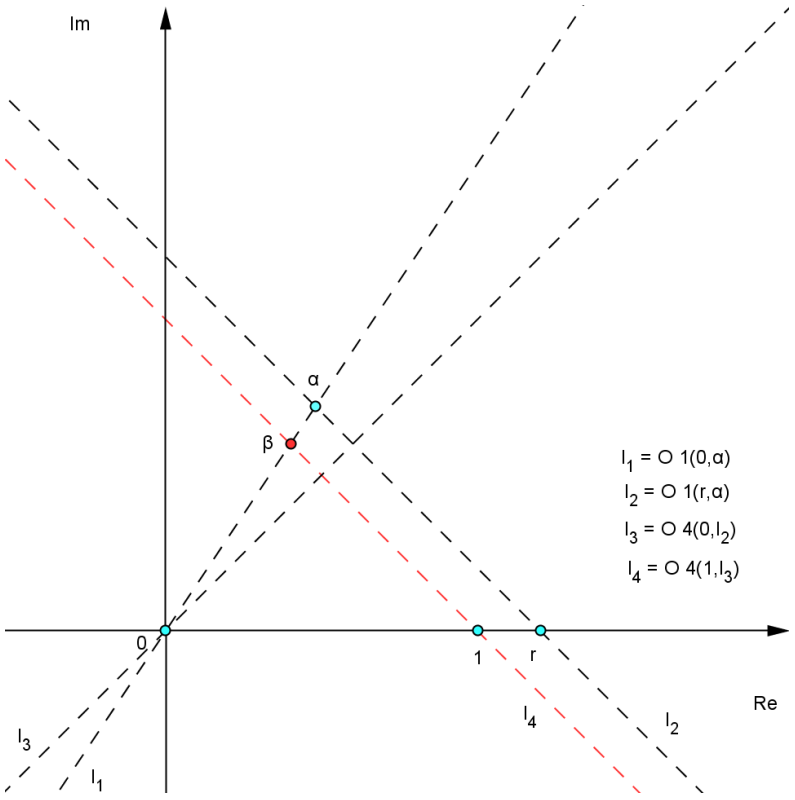
Det er altså mulig å multiplisere med reelle tall i origami.

Multiplikasjon med i er bare det samme som å kunne rotere et reellt tall 90 grader.



Figur 28 Multiplikasjon med *i*

Brettingen er helt lik brettingen i ***Figur 17***. Dermed er det mulig å multiplisere sammen tall i origami. Til slutt vil vi vise divisjon. Generelt er $(a + ib)^{-1} = a - ib/a^2 + b^2$. Det eneste vi trenger å vise er at det er mulig å dele et origamitall med et reelt tall. Gjentar som for multiplikasjon:



Figur 29 Divisjon av reelle tall i origami

Fra formlike trekanter får vi:

$$\frac{|\alpha|}{r} = \frac{|\beta|}{1} \Leftrightarrow |\beta| = r^{-1}|\alpha|, \text{ der } r > 0$$

Dermed har vi vist at origamitallene $\mathcal{O}$ danner en kropp. Til slutt skal vi vise at $\alpha \in \mathcal{O} \Rightarrow \sqrt[3]{\alpha} \in \mathcal{O}$. Vi skriver α på polarform: $\sqrt[3]{\alpha} = \omega^i \sqrt[3]{r} e^{i\theta/3}$, hvor $r = |\alpha| > 0$. ω^i må være med slik at polynomet splitter fullstendig over $\mathcal{O}$. Vi kan tredele θ ved ***Figur 18***. For å brette $\sqrt[3]{r}$ kan vi bare bruke parablene i ***Eksempel 4*** hvor $a = 0$ og $b = -r$. Da får vi brennpunktene F_1, F_2 og direktrisene D_1, D_2. Vi finner simultantangenten T til parablene ved å bruke $\mathcal{O}$ 6 på brennpunktene og direktrisene. Da vil stigningstallet m til T være gitt ved $m = \sqrt[3]{r}$. Ettersom $\mathcal{O}$ er en kropp, så vil $\sqrt[3]{r} \in \mathcal{O}$. Videre er $\omega = e^{2\pi i} \in \mathcal{O}$. Da følger det at $\sqrt[3]{\alpha} = \omega^i \sqrt[3]{r} e^{i\theta/3} \in \mathcal{O}$, $i = 0,1,2$.

■

Man kan ved Galoisteorien vise følgende resultat for origamitallene:

Teorem 11.: La $\alpha \in \mathbb{C}$ være algebraisk over $\mathbb{Q}$ og la $\mathbb{Q} \subset L$ være en splittekropp av minimalpolynomet av α over $\mathbb{Q}$. Da er α et origamitall hvis, og bare hvis, $[L:\mathbb{Q}] = 2^a 3^b$, der $a \, og \, b$ er heltall som er større eller lik 0.

I ***Eksempel 2.4*** fant vi ut at Galois gruppen til $L = \mathbb{Q}\left[\sqrt[3]{2}, \omega\right]$. Nå vil vi gjerne finne ut om vi kunne ha konstruert L med origami.

Eksempel 5.: La $\alpha \in L = \mathbb{Q}\left[\sqrt[3]{2}, \omega\right]$. Vi vil finne ut om α er et origamitall. Ifølge ***Teorem 11.*** ,så er α et origamitall hvis, og bare hvis, splittekroppen L' til minimalpolynomet til α kan skrives på formen $[L':\mathbb{Q}] = 2^a 3^b$. I ***Eksempel 2.2*** fant vi ut at L er en normal utvidelse. Da følger det at splittekroppen L' må ligge i L. Lagranges teorem (***Teorem 18***) viser da at: $[L':\mathbb{Q}]|[L:\mathbb{Q}]$. Ettersom $[L:\mathbb{Q}]$ er av grad 6, så kan graden på splittekroppen skrives som $[L':\mathbb{Q}] = 2^a 3^b$. Det betyr at $L = \mathbb{Q}\left[\sqrt[3]{2}, \omega\right]$ kan konstrueres ved hjelp av origami.

Til slutt vil vi som lovt vise at også kubens fordobling lar seg løse ved origami.

Korollar 3.: La $f(x) \in \mathbb{Q}[x]$ være et polynom av grad ≤ 4. Da er røttene av $f(x)$ origamitall, det vil si, vi kan løse $f(x) = 0$ ved origami.

Bevis: La $f(x) \in F[x]$ være et irredusibelt monisk polynom[16] av grad 4. Planen er nå å finne splittekroppen til et minimalpolynom av grad 4. Vi tar et element α, slik at $F = \mathbb{Q} \ni \alpha$, men $F \not\ni \sqrt[4]{\alpha}$ og $L \ni \sqrt[4]{\alpha}$. Utvidelsen $F \subset L$ er splittekroppen til minimalpolynomet $x^4 - \alpha$, som har to reelle og to komplekse røtter. La $\omega = e^{2\pi i/4}$, vi kan vise at $L = \mathbb{Q}[\sqrt[4]{\alpha}, \omega]$ er en normal utvidelse (på samme måte som vi gjorde i ***Eksempel 2.2***). Det kan vises at for splittekroppen til et polynomav grad n, så kan vi se på Galoisgruppen som en undergruppe av S_n, (se kapittel 6.3 side 133 i [6]). Symmetrigruppen S_n har orden $n!$ (kapittel 8 side 78 i [7]). Finner graden til utvidelsen $[L:\mathbb{Q}] = 8$ (kan gjøres på samme måte som vi gjorde i ***Eksempel 2.3***). Da ser vi, som vi vet fra Lagranges teorem, at:$\left|Gal(\mathbb{Q}[\sqrt[4]{\alpha}, \omega]/\mathbb{Q})\right| = 8$ deler $4! = 24$. Ettersom graden av splittekroppen deler 24, så må den være på formen $2^a 3^b$. Vi kan gå fram på samme måte for polynomer av tredje grad.■

[16] Teknisk sett må polynomet også være separabelt. Men over en kropp med karakterestikk 0, så er ethvert irredusibelt polynom separabelt. Dette er fordi vi kan kvitte oss med multiple røtter (for eksempel ved $f/\gcd(f', f)$).

Fra resultatet over kan vi konkludere:

Kubens fordobling.: Ifølge ***Korollar 3*** kan vi nå løse problemet med kubens fordobling ved origami.

Når det gjelder problemet med sirkelens kvadratur, så husker vi at π er transcendental over $\mathbb{Q}$. Det betyr at π ikke er i en endelig kroppsututvidelse av $\mathbb{Q}$. Med andre ord vil problemet med sirkelens kvadratur forbli uløselig hvis en fortsetter å bruke den framgangsmetoden vi har brukt (studere endelige utvidelser av $\mathbb{Q}$).

6.3. Referanser og valg av referanser

Cox har en flott redgjørelse av origami i sin bok. En annen forfatter – James King, viser eksplisitt at origamitallene oppfyller kroppsaksiomene. Denne artikkelen er ikke publisert, men det er mulig å laste ned dokumentet som pdf fra internett. G.E. Martin har også en fin og detaljert redgjørelse av origami. Robert Lang har skrevet flere bøker om origami, der han blant annet viser til anvendelser av origami i fagfelter som romfart og medisin.

(1) *Famous Mathematics Quotes*:

http://www.math.okstate.edu/~wli/teach/fmq.html

(6) Cox, D.A. (2004). *Galois Theory.* New Jersey: Wiley.

(7) Fraleigh, J.B. (2003). *A First Course In Abstract Algebra.* Rhode Island:

Pearson Education.

(8) King, J. (2004). *Origami – Constructible Numbers*.

(9) G.E. Martin (1998), *Geometric Constructions*, New York, Berlin, Heidelberg: Springer-

Verlag.

(10) R.J.Lang, *Origami: Complexity in Creases (Again)*:

http://eands.caltech.edu/articles/LXVII1/origami.html

(11) R.A.Adams (2003), *Calculus A Complete Course – fifth edition*, Toronto, Ontario:

Addison Wesly Longman.

7. Tillegg

"What we know is not much. What we do not know is immense."

Pierre-Simon Laplace (1749-1827)

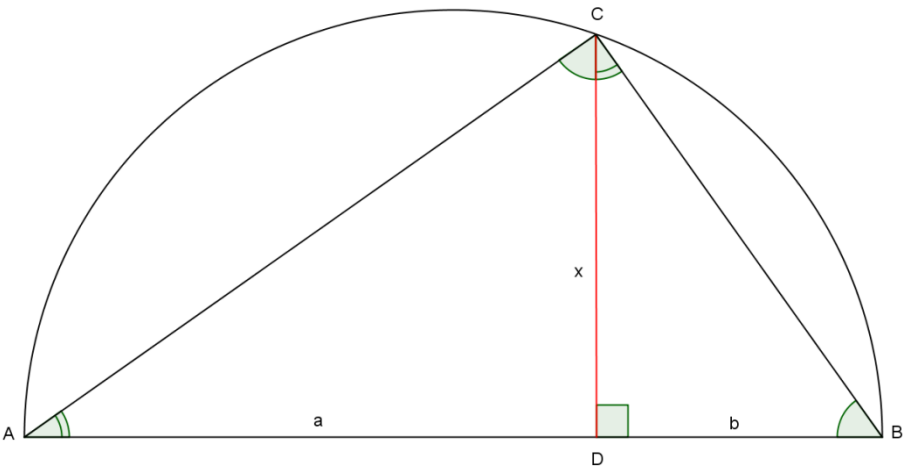
7.1. Enkel mellomproporsjonal

I dette avsnittet skal vi snakke litt om proporsjonalitet. De greske matematikerne forsøkte med dette konseptet å komme nærmere de irrasjonalle tallene.

Definisjon 9.: *Mellomproporsjonalen* mellom to positive tall a og b er et positivt tall x, slik at

$$\frac{a}{x} = \frac{x}{b}$$

En generell konstruksjon som gir mellomproporsjonalen, er gitt under:



Figur 30 Konstruksjon av enkel mellomproporsjoanl

7.2. Litt om grupper

Oppgaven er hovedsakelig myntet på dem som har litt kjennskap til moderne algebra. For å repetere litt tidligere kunnskaper: Hva er egentlig en gruppe? En gruppe er en mengde av objekter G sammen med en operator $*$, som setter sammen to elementer a og b til et nytt element, nemlig $a * b$. Vi kaller gjerne denne operatoren for en binær operator. For å kunne kvalifiseres som en gruppe $(G,*)$, så må mengden av objekter og operatoren oppfylle noen krav som vi kaller for gruppeaksiomene.

G.1 For alle a, b i G, så må resultatet $a * b$ også være i G (**Lukket**).

G.2 For alle a, b og c i G, så $(a * b) * c = a * (b * c)$ (**Assosiativitet**).

G.3 Det må eksistere et element e i G, slik at for hvert element a i G så holder ligningen: $e * a = a * e = a$ (**Identitetselement**).

G.4 For hver a i G, så eksisterer det et element b slik at $a * b = b * a = 1$ (**invers element**).

Idéen om grupper kommer naturlig som følge av vårt ønske om å løse ligninger. La oss se på et eksempel:

Eksempel 6.: Ønsket er å løse ligningen $5 + x = 2$. Det betyr at addisjon er den binære operatoren og at $\mathbb{Z}$ er mengden G. Slik er det vi egentlig løser denne ligningen: (Legg merke til hvordan aksiomene blir brukt)

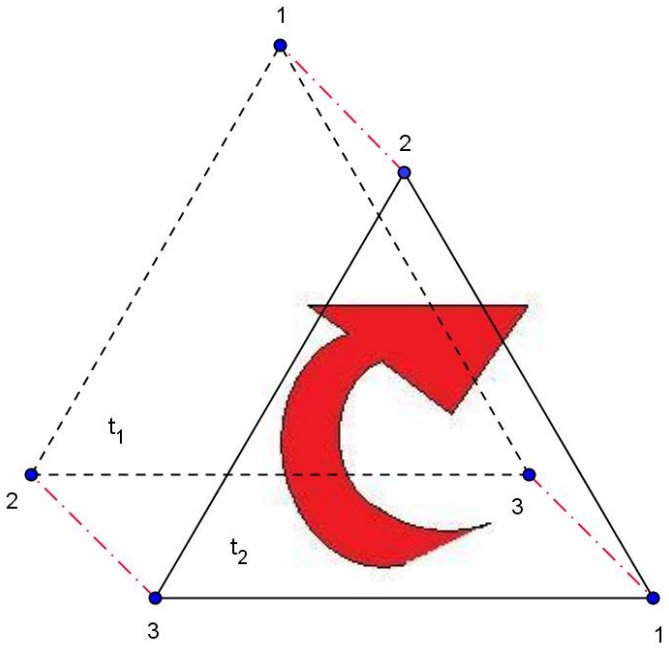
$$5 + x = 2, \text{ gitt}$$
$$-5 + (5 + x) = -5 + 2, \text{ legger til } -5$$
$$(-5 + 5) + x = -5 + 2, \text{ Assosiativitet}$$
$$0 + x = -5 + 2, \text{ legger sammen } -5 + 5$$
$$x = -5 + 2, \text{ egenskap av } 0$$
$$x = -3, \text{ legger sammen } -5 + 2$$

Dette betyr at heltallene sammen med addisjon utgjør en gruppe, altså $(\mathbb{Z}, +)$.

Dette kan kanskje virke tungvint. Vi vet jo hvordan vi skal løse en slik ligning, men grupper kan være svært forskjellig fra eksempelet over. En gruppe behøver for eksempel ikke å bestå av tall. Likevel kan en oppdage når en gjør den litt mer tungvinte fremgangsmetoden, at mengdene av kanskje vidt forksjellige objekter viser seg å være den samme mengden av objekter eller at de har den samme strukturen. Det er bare en forskjell i navn eller symboler. Vi sier at to slike strukturer er *isomorfe*. I mange grupper er det slik at elementene er transformasjoner av et objekt og den binære operatoren blir

betraktet som funksjonskomposisjon. La oss se på et eksempel hvor gruppen består av symmetrier, en såkalt permutasjonsgruppe.

Eksempel 7.: I dette eksempelet skal vi lage en tabell over funksjonskomposisjoner av automorfier til en likesidet trekant. Hva betyr automorfier til en trekant? Se for deg en trekant t_1 der vi kaller kantene for 1,2 og 3. Nå lager vi en helt identisk trekant t_2, som vi legger over t_1. Automorfiene til trekanten er alle måtene vi kan snu og vende på t_1, slik at kantene på t_1 ligger rett over kantene til t_2 (se **Figur 20.**).

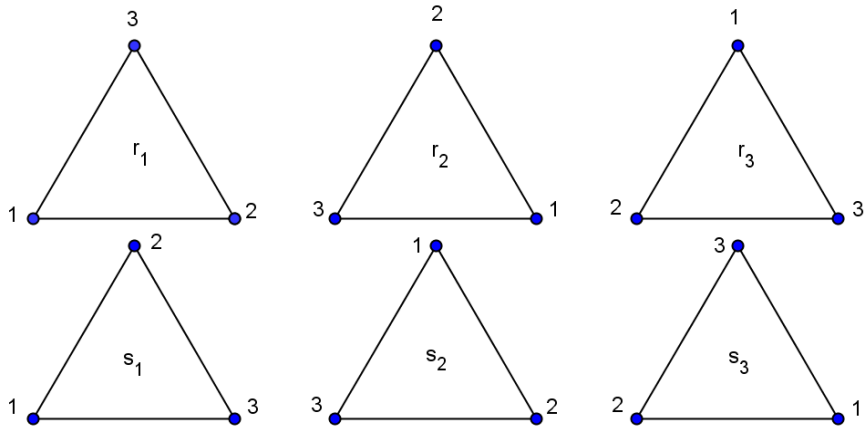


Figur 31 En automorfi til en likesidet trekant

Hvor mange automorfier er det? La oss sjekke! Vi lar r_i stå for rotasjoner og s_i for speilinger.

Rotasjoner:

Speilinger:



Figur 32 Automorfier til en likesidet trekant

Vi kan skrive dette på følgende måte

$$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$
$$r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Hva er for eksempel $s_1 \circ s_2$ og $r_3 \circ s_2$?

$$s_1 \circ s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = r_3$$
$$r_3 \circ s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = s_1$$

Vi fører resultatene opp i en tabell.

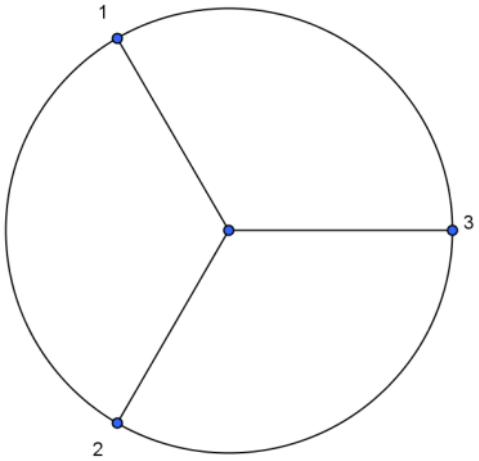
∘	r_1	r_2	r_3	s_1	s_2	s_3
r_1	r_1	r_2	r_3	s_1	s_2	s_3
r_2	r_2	r_3	r_1	s_3	s_1	s_2
r_3	r_3	r_1	r_2	s_2	s_3	s_1
s_1	s_1	s_2	s_3	r_1	r_2	r_3
s_2	s_2	s_3	s_1	r_3	r_1	r_2
s_3	s_3	s_1	s_2	r_2	r_3	r_1

Tabell 2 Permutasjons multiplikasjonstabell

Ser du noen likheter mellom ***Tabell 1*** og ***Tabell 2***? Hva betyr det?

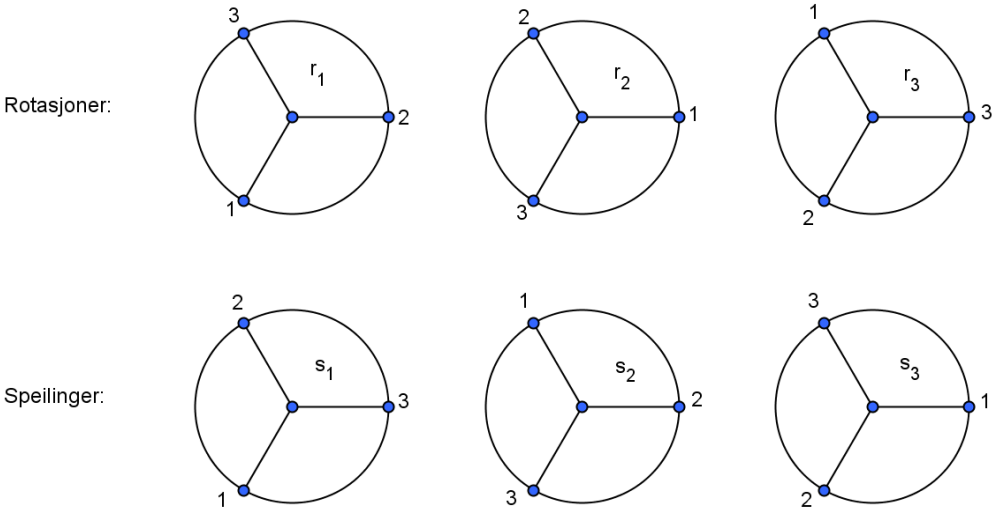
La oss se på et annet eksempel til der vi studerer permutasjoner.

Eksempel 8.: Figuren vi skal studere, er en vi er godt kjent med – sirklen. La oss dele den i tre deler, som vist i figuren under.



Figur 33 Hvilke automorfier kan vi få ut fra denne sirklen?

Vi gjentar prosedyren som i forrige eksempel og finner:



Figur 34 Automorfier til en tredelt sirkel

Vi ser at hvis vi hadde laget en tabell med permutasjoner som i ***Eksempel 5***, så ville den bli helt lik ***Tabell 2*****.** Det betyr at de to gruppene er isomorfe.

Det siste jeg vil nevne om gruppeteorien, er normale undergrupper. Da er det nødvendig å innføre et begrep som kanskje mange synes er litt vanskelig, nemlig *kosett*. Definisjonen er gitt under. Men først vil jeg si noe om notasjon. Hvis g og h er elementer i en gruppe, så er det vanlig å skrive gH istedenfor $g * H$.

Definisjon 10.: La G være en gruppe og H en undergruppe av G, og la g være et element i G.

$$gH = \{gh | h \in H\}$$

Blir kalt et venstre *kosett* av H i G.

La oss se på et eksempel for bedre å forstå denne definisjonen.

Eksempel 9.: La G være gruppen av heltall med addisjon, altså $(\mathbb{Z}, +)$.

$6\mathbb{Z}$ er en undergruppe av $\mathbb{Z}$, så vi lar dette være H. Hvis vi lar g være elementet 2 i G, da blir kosettet:

$$gH = 2 + 6\mathbb{Z} = \{2 + h | h \in 6\mathbb{Z}\} =$$
$$\{\dots, 2 + (-12), 2 + (-6), 2 + 0, 2 + 6, 2 + 12, \dots\} =$$
$$\{\dots, -10, -4, 2, 8, 14, \dots\}$$

Venstre kosett skrives som gH. En kan på samme måte definere høyre kosett av H i G.

$$Hg = \{hg | h \in H\}$$

Venstre og høyre kosett trenger ikke å være den samme mengden. Men for alle abelske grupper er de lik. Med det i tankene, passer det å komme med følgende definisjon:

Definisjon 11.: La G være en gruppe og H en undergruppe. Vi sier at H er en *normal undergruppe*, hvis mengdene til det venstre og høyre kosettet av H i G sammenfaller (eller er like).

Følgende teorem kan brukes for å avgjøre om en undergruppe er en normal undergruppe.

Teorem 12.: De følgende betingelsene er ekvivalente for en undergruppe H av en gruppe G, for at H skal være en normal undergruppe av G.

- $ghg^{-1} \in G$ for alle $g \in G$ og $h \in H$.
- $gHg^{-1} = H$ for alle $g \in G$.
- $gH = Hg$ for alle $g \in G$.

Betingelse nummer to i dette teoremet blir ofte brukt som definisjonen av en normal undergruppe H av en gruppe G. Nå vil vi komme med en definisjon som forklarer hvorfor normale undergrupper er så interessante.

Definisjon 12.: La G være en gruppe og H en normal undergruppe. Da er gruppen

$$G/H = \{gH | g \in G\}$$

Faktorguppen G modulo H.

Elementene i G/H er kosett av H i G. Et eksempel på en faktorgruppe er $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Kosettene er elementene i gruppen $\mathbb{Z}_n$, der elementene i $\mathbb{Z}_n$ representerer mengden av heltall som gir samme rest ved divisjon av n. La oss drøfte et eksempel for å forsøke og forstå dette litt bedre.

Eksempel 10.: Vi ser på faktorgruppen $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.
La $n = 6$. Da består vår mengde av følgende elementer (kosett).

$\{\dots, -12, -6, 0, 6, 12, \dots\}$:Rest 0 ved divisjon av 6
$\{\dots, -11, -5, 1, 7, 13, \dots\}$:Rest 1 ved divisjon av 6
$\{\dots, -10, -4, 2, 8, 14, \dots\}$:Rest 2 ved divisjon av 6
$\{\dots, -9, -3, 3, 9, 15, \dots\}$:Rest 3 ved divisjon av 6
$\{\dots, -8, -2, 4, 10, 16, \dots\}$:Rest 4 ved divisjon av 6
$\{\dots, -7, -1, 5, 11, 17, \dots\}$:Rest 5 ved divisjon av 6

Vi kan representere hvert av disse elementene (som egentlig er en mengde) i denne mengden som restleddet, altså som et heltall mellom 0 og 5. For eksempel vil tallet 3 i $\mathbb{Z}_6 = \{0, 1, \dots, 5\}$, representere alle heltall med rest 3 ved divisjon av 6.

La oss dvele litt ved denne gruppen, altså $(\mathbb{Z}_6, +)$. Siden addisjon er vår operator, så er gruppen abelsk og vi lar 0 være vårt identitetselement. Vi ser at $2 + 2 = 4$, men hva med $3 + 4$? Tallet 7 finnes jo ikke i denne mengden, men det blir lik 1. Husk at elementene 3 og 4 ikke egentlig er tallene 3 og 4, men at de representerer alle tall med rest 3 og 4 ved divsjon av 6. Vi ser at $3 + 4 = 7$ gir 1 som rest ved divisjon av 6. Legg også merke til at tallet 1 representerer elementet $\{\dots, -11, -5, 1, 7, 13, \dots\}$, og 7 er i samme ekvivalensklasse som 1. Er ikke dette fantastisk? Til slutt kan vi se på denne gruppens cayley- tabell[17].

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Tabell 3 Cayley tabell til $\mathbb{Z}_6$

Se på den fine symmetrien! Ettersom tabellen er symetrisk om diagonalen (fra topp til bunn), så betyr det at gruppen er abelsk.

Grunnen til at G/H kalles faktorgruppen eller kvotientgruppen, har med divisjon av heltall å gjøre. Hvis en deler 15 på 3 så blir svaret 5, ettersom en kan gruppere 15 objekter inn i 3 delmengder som hver inneholder 5 objekter. Med faktorgruppen er det den samme idéen, forskjellen er at en ender opp med en gruppe som svar istedenfor et tall. Det er fordi en gruppe har mer struktur enn en vilkårlig mengde av objekter.

7.3. Litt om kropper

Vi snakker en god del om kropper i denne oppgaven, så det er fint om en har en klar forståelse av hva dette kanskje litt difuse begrepet egentlig betyr. Kropper kan bli betraktet som grupper, men med en ekstra binær operator og noen tilleggsaksiomer. En kropp er altså en algebraisk struktur, der addisjon, subtraksjon, divisjon og multiplikasjon må være tillatt og oppfylle følgende aksiomer:

$\mathscr{K}1$ F må være **lukket under addisjon og multiplikasjon**. Altså for alle $a, b \in F$, så må $a + b$ og ab være i F.

[17] Cayley- tabeller beskriver strukturen av en endelig gruppe. En kan finne ut en rekke ting ved å studere slike, som for eksempel om gruppen er abelsk eller ikke.

$\mathscr{K}2$ **Addisjon og multiplikasjon må være assosiativ**. Det vil si for alle a, b, c i F, så har vi $a + (b + c) = (a + b) + c$ og $a(bc) = (ab)c$.

$\mathscr{K}3$ **Addisjon og multiplikasjon er kommutativ**. $a + b = b + a$ og $ab = ba$.

$\mathscr{K}4$ **Additiv og multiplikativ identitet**. Additiv: $a + 0 = a$, multiplikativ: $a \cdot 1 = a$.

$\mathscr{K}5$ **Additiv og multiplikativ invers**. Additiv: $a + (-a) = 0$, multiplikativ: $a \cdot (a^{-1}) = 1$, $a^{-1} \neq 0$. (Med andre ord så må divisjon og subtraksjon eksistere).

$\mathscr{K}6$ **Addisjon og multiplikasjon er distributativ**. For alle a, b, c i F gjelder $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

De vanligste kroppene er de reelle tallene ($\mathbb{R}$), de komplekse tallene ($\mathbb{C}$) og de rasjonelle tallene ($\mathbb{Q}$). $\mathbb{Z}$ er ikke en kropp! Kan du se hvorfor?

Eksempel 11.: De rasjonelle tallene $\mathbb{Q}$, som består av elementer på formen $\frac{a}{b}$, hvor $b \neq 0$ er en kropp. Vi ser at den additive inversen bare er $-\frac{a}{b}$ og den multiplikative inversen er $\frac{b}{a}$. De andre aksiomene (som distributivitet, kommutativitet og assosiativitet), reduseres bare til standardegenskaper ved de rasjonelle tallene.

$$\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{cf + ed}{df} = \frac{a(cf + ed)}{bdf} = \frac{acf}{bdf} + \frac{aed}{bdf} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$$

Vi kan også lage en kropp som er nokså annerledes fra det forrige eksempelet.

Eksempel 12.: Vi lar denne kroppen bestå av fire elementer: O, I, A og B. Videre lar vi O være det additive identitetselementet og I er det multiplikative identitetselementet.

·	O	I	A	B
O	O	O	O	O
I	O	I	A	B
A	O	A	B	I
B	O	A	I	A

+	O	I	A	B
O	O	I	A	B
I	I	O	B	A
A	A	B	O	I
B	B	A	I	O

Tabell 4 Operatorene for kroppen

En kan sjekke om kroppsaksiomene holder, for eksempel:

$A \cdot (B + A) = A \cdot I = A$ som er lik $A \cdot B + A \cdot A = I + B = A$, som viser distributivitet. Denne kroppen er et eksempel på en endelig kropp med 4 elementer.

7.4. Noen nyttige teoremer og resultater

I dette avsnittet vil jeg gi noen teoremer og resultater som trolig er kjente, men godt å huske på når en leser gjennom denne oppgaven.

Definisjon 13.: Et ikke- konstant polynom $f(x) \in F[x]$, er *irredusibel over* F eller er et irredusibelt polynom i $F[x]$ hvis $f(x)$ ikke kan bli uttrykt som et produkt $g(x)h(x)$ av to polynomer $g(x)$ og $h(x)$ i $F[x]$, begge av lavere grad enn $f(x)$. Hvis $f(x) \in F[x]$ er et ikke- konstant polynom som ikke er irredusibel over F, da er $f(x)$ *redusibel over* F.

Definisjon 14.: Et element α fra en kroppsutvidelse E av en kropp F, er algebraisk over F, hvis f(α) = 0 for en eller annen ikke- konstant funksjon $f(x) \in F[x]$.

Definisjon 15.: Minimalpolynomet av α, er det er det moniske polynomet p (monisk polynom betyr bare at koeffisienten foran leddet av høyest grad er lik 1), med koeffisienter i F, av minste grad slik at $p(\alpha) = 0$. Minimalpolynomet er dessuten irredusibel over F.

Definisjon 16.: De konjugerte elementene til et algebraisk element α, over en kropp F, er de (andre) røttene til minimal polynomet p av α over F.

Definisjon 17.: Det n-te syklotomiske polynomet, for ethvert positivt heltall n, er det moniske polynomet:

$$\phi_n(x) = \prod_{\omega} (x - \omega)$$

Teorem 13.: Hvis $f(x) \in \mathbb{Z}[x]$, da vil $f(x)$faktoriseres til et produkt av to polynomer av lavere grad r og s i $\mathbb{Q}$[x] hvis, og bare hvis, den har en slik faktorisering med polynomer av samme grad r og s i $f(x)$.

Korollar 4.: Hvis $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ er i $\mathbb{Z}$[x] der $a_0 \neq 0$, og hvis $f(x)$ har en rot i $\mathbb{Q}$, da har den en rot m i $\mathbb{Z}$, der m$|a_0$.

Det neste teoremet, er det berømte Schönemann-Eisenstein- kriteriet. Teoremet blir ofte bare kalt "Eisenstein- kriteriet", men en bør også nevne Schönemann ettersom han beviste teoremet først i 1846, og Eisenstein beviste det uavhengig av Schönemann i 1850[18].

Teorem 14.: La $p \in \mathbb{Z}$ være primtall. Anta at $f(x) = a_n x^n + \cdots + a_0$ er i $\mathbb{Z}[x]$, og at $p \nmid a_n$, men $p|a_i$ for alle $i < n$, der $p^2 \nmid a_0$. Da er $f(x)$ irredusibel over $\mathbb{Q}$.

Teorem 15.: Alle ω^k, $1 \leq k \leq m$, $(k, m) = 1$, er konjugerte av ω.

Teorem 16.: La E være en kroppsutvidelse av F, og la $\alpha \in E$ være algebraisk over F. Hvis $\deg(\alpha, F) = n$, da er $F(\alpha)$ et n dimensjonalt vektorrom over F med basis $\{1, \alpha, \dots, \alpha^{n-1}\}$.

Teorem 17.: Hvis E er en endelig kroppsutvidelse av en kropp F, og K er en endelig kroppsutvidelse av E, da er K en endelig kroppsutvidelse av F og

$$[K:F] = [K:E][E:F]$$

Teorem 18.: La H være en undergruppe av en endelig gruppe G. Da vil ordenen av H være en divisor av ordenen til G.

Til slutt vil jeg gjerne gi en liten tabell, som kan være litt til hjelp når en jobber med Galoisgruppene.

1	primtall 2	primtall 3	4	primtall 5	6	primtall 7	8	9	10
e	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_4$	$\mathbb{Z}_5$	$\mathbb{Z}_6$	$\mathbb{Z}_7$	$\mathbb{Z}_8$	$\mathbb{Z}_9$	$\mathbb{Z}_{10}$
			$\mathbb{Z}_2 \times \mathbb{Z}_2$		S_3		$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_3 \times \mathbb{Z}_3$	D_5
					D_3		$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$		
							D_4		

Tabell 5 Liste over mulige grupper opp til orden 10 (De abstrakte gruppene, det finnes jo uendlig mange grupper, de enkelte av disse kalles gjerne de konkrete gruppene)

[18] For mer detaljer se [6] side 87

7.5. Litt om valg av Kronologi

Ordet *kronologi* kommer fra det greske ordet *khronologia* (sammensatt av *khronos* som betyr ”tid” og *logia*, av *logos* som betyr ”ord, tale, tanke”). Kronologi betegner læren eller vitenskapen om tidsregning og tidsinndeling. Kronologi gjør det mulig å plassere begivenheter i riktig rekkefølge og sette dem i den rette sammenheng i forhold til hverandre, og dessuten tidfeste bestemte hendelser. Det å bruke en tidsregning med utgangspunkt i en viktig hendelse ble innført relativt sent. Grekernes tidsregning, som en antar å være det eldste eksempel på en slik måte å regne tiden på, antar man først ble tatt i bruk på 300-tallet f.v.t. Grekerne inndelte tiden i perioder på fire år, olympiader, med utgangspunkt i den første olympiaden, som man mener startet i 776 f.v.t. De angav ofte også de enkelte år ved henvise til bestemte myndighetspersoners embetsperioder.

Først på 500-tallet e.v.t. foretok munken Dionysius Exiguus en beregning som dannet grunnlaget for en tidsregning med utgangspunkt i Kristi fødsel, den tidsregning som nå i alminnelighet brukes i den vestlige verden. For å gjøre en lang historie kort, så er denne tidsregningen ikke helt nøyaktig! Det viser seg at Jesus ble født ca. 2 f.v.t. (altså år 2 f.Kr). Interesserte lesere kan finne flere detaljer rundt dette blant annet i bøkene ”*The Bearing of Recent Discovery on the Trustworthiness of the New Testament*” av W.Ramsay, 1979, s.285, 291 og ”*Dictionnaire du Nouveau Testament*” i Crampons franske bibeloversettelse (1939-utg., s.360).

7.6. Referanser og valg av referanser

Daniel A. Marcus har en fin behandlig av tallteori. Flere forelesere på universitet liker denne, særlig fordi den er skrevet på en slik interaktiv måte. En blir hele tiden oppfordret til å sjekke at utsagnene han kommer med, er sanne. En kan også finne mange fine og enkle eksempler om abstrakt algebra på Wikipedia.

(1) *Famous Mathematics Quotes*:

http://www.math.okstate.edu/~wli/teach/fmq.html

(8) Fraleigh, J.B. (2003). *A First Course In Abstract Algebra.* Rhode Island:

Pearson Education

(12) Marcus, D.A. (1977). *Number Fields.* Michigan: Springer